

Apparatus and process for verifying honest gaming transactions over a communications network

Publication number: JP2001514909 (T)

Publication date: 2001-09-18

Inventor(s):

Applicant(s):

Classification:



- international: **A63F13/12; A63F13/00; G06Q50/00; G07F17/32; A63F13/12; A63F13/00; G06Q50/00; G07F17/32; (IPC1-7): A63F13/12; A63F13/00; G06F17/60**

- European: G07F17/32D

Application number: JP20000509065T 19980901

Priority number(s): US19970921520 19970902; WO1998US18047 19980901

Also published as:

 JP4087557 (B2)
 US6165072 (A)
 US6030288 (A)
 WO9912135 (A1)
 WO9912135 (A8)

more >>

Abstract not available for JP 2001514909 (T)

Abstract of corresponding document: **US 6165072 (A)**

Apparatus and method for verifying honest gaming transactions over a communications network includes structure and process whereby a host processor receives a random number from a satellite processor over the communications network. The host processor generates a game seed based on the random number. The host processor also receives an arbitrary game input from the satellite processor and generates a game result based on the game input, the game seed, and predetermined game rules. The satellite processor provides the random number and the arbitrary game input to the host processor over the communications network, and receives data corresponding to the game seed and the game result from the host processor. The satellite processor verifies the honesty of the transaction by (i) generating a game result based on the game input, the data corresponding to the game seed, and the predetermined game rules, and (ii) compares the generated game result with the received game result. A storage medium is also provided for storing a computer-implemented program to carry out the functions described above.

Data supplied from the **esp@cenet** database — Worldwide

(51)Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
A 6 3 F 13/12		A 6 3 F 13/12	C 2 C 0 0 1
13/00		13/00	A 5 B 0 4 9
G 0 6 F 17/60	1 4 8	G 0 6 F 17/60	1 4 8

審査請求 未請求 予備審査請求 有 (全 93 頁)

(21)出願番号	特願2000-509065(P2000-509065)	(71)出願人	クイックソティック ソリューションズ インク。
(86) (22)出願日	平成10年9月1日(1998.9.1)		アメリカ合衆国、20009 ワシントン、デ
(85)翻訳文提出日	平成12年3月2日(2000.3.2)		イーシー、シックスティーンズ ストリ
(86)国際出願番号	P C T / U S 9 8 / 1 8 0 4 7		ト、エヌ.ダヴリュ., 1837
(87)国際公開番号	W O 9 9 / 1 2 1 3 5	(72)発明者	デイヴィス, スティーヴン, ベンジャミン
(87)国際公開日	平成11年3月11日(1999.3.11)		アメリカ合衆国、20024 ワシントン、デ
(31)優先権主張番号	0 8 / 9 2 1 , 5 2 0		イーシー, エム ストリート エス.ダヴ
(32)優先日	平成9年9月2日(1997.9.2)		リュ. ナンバー507ダヴリュ 490
(33)優先権主張国	米国 (U S)	(74)代理人	弁理士 岡部 正夫 (外12名)
		最終頁に続く	

(54)【発明の名称】 通信ネットワークを通しての公正なゲーム進行手続を確保するための装置およびプロセス

(57)【要約】
それにより、ホスト・プロセッサが、通信ネットワークを通して衛星プロセッサから乱数を受信する構造体およびプロセスを含む通信ネットワークを通して、不公正な行為のないゲーム実行取引を確認するための装置および方法。ホスト・プロセッサは、上記乱数に基づいて、ゲーム・シードを発生する。ホスト・プロセッサは、また、上記衛星プロセスから任意のゲーム入力を受信し、上記ゲーム入力、上記ゲーム・シード、および予め定めたゲームの規則に基づいて、ゲームの結果を発生する。衛星プロセッサは上記乱数および上記任意のゲーム入力を、通信ネットワークを通して、ホスト・プロセッサに供給し、ホスト・プロセッサから、上記ゲーム・シードおよび上記ゲームの結果に対応するデータを受信する。衛星プロセッサは、(i) 上記ゲーム入力、上記ゲーム・シードに対応する上記データ、および上記予め定めたゲームの規則に基づいて、ゲームの結果を発生し、(i i) 上記の発生したゲームの結果を上記の受信したゲームの結果と比較することにより、上記取引に不公正な行為がないことを確認する。上記機能を行うために、コ

ンピュータが実行するプログラムを記憶するための記憶媒体も設置される。

【特許請求の範囲】

【請求項1】 通信ネットワークを通して、公正なゲーム進行手順を確保するための装置であって、

ゲーム・シードを発生するためのホスト・プロセッサであり、衛星プロセッサからゲーム入力を受信し、前記ゲーム入力、ゲーム・シード、および予め定めたゲームの規則から、ゲームの結果を発生し、前記ゲーム・シードおよび前記ゲームの結果を前記衛星プロセッサに送信するホスト・プロセッサと、

前記通信ネットワークを通して、前記ゲーム入力を供給し、前記ホスト・プロセッサから、前記ゲーム・シードおよび前記ゲームの結果を受信し、(i) 前記ゲーム入力、前記ゲーム・シード、および前記の予め定めゲームの規則に基づいて、ゲームの結果を発生し、(ii) 前記の発生したゲームの結果を、前記の受信したゲームの結果とを比較するための衛星プロセッサとを備える装置。

【請求項2】 請求項1に記載の装置において、前記衛星プロセッサが、前記ゲーム・シードを発生するために、前記ホスト・プロセッサが使用する衛星乱数を供給する装置。

【請求項3】 請求項1に記載の装置において、前記ホスト・プロセッサが、前記ゲーム・シードを発生するために、前記ホスト・プロセッサが使用するホスト乱数を発生する装置。

【請求項4】 請求項3に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数からホスト変形を発生し、前記ホスト変形を前記衛星プロセッサに供給する装置。

【請求項5】 請求項4に記載の装置において、前記ホスト・プロセッサが、前記衛星プロセッサに、前記ホスト乱数を供給し、前記衛星プロセッサが、前記ホスト変形が供給したホスト乱数から発生したものであることを確認するために、前記ホスト乱数および前記ホスト変形を使用する装置。

【請求項6】 請求項5に記載の装置において、前記衛星プロセッサが、前記ホスト乱数から前記ゲーム・シードを発生する装置。

【請求項7】 請求項4に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数の非可逆的変形から前記ホスト乱数を計算する装置。

【請求項 8】 通信ネットワークを通して、合作のランダム出力を生成するための装置であって、

ホスト乱数を発生するためのホスト・プロセッサであり、衛星プロセッサから衛星乱数を受信し、前記衛星乱数、および前記ホスト乱数に基づいて、協力ランダム出力を発生するホスト・プロセッサと、

前記衛星乱数を発生し、前記通信ネットワークを通して、前記衛星乱数を前記ホスト・プロセッサに供給するための衛星プロセッサとを備える装置。

【請求項 9】 請求項 8 に記載の装置において、前記ホスト・プロセッサが、ゲーム・シードを発生するために、前記協力ランダム出力を使用する装置。

【請求項 10】 請求項 8 に記載の装置において、前記ホスト・プロセッサが、前記通信ネットワークを通して、前記衛星プロセッサに前記ホスト乱数を供給し、前記衛星プロセッサが、前記協力ランダム出力を確認するために、前記衛星乱数および前記ホスト乱数を使用する装置。

【請求項 11】 請求項 8 に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数からホスト変形を発生し、前記ホスト変形を、前記通信ネットワークを通して、前記衛星プロセッサに供給し、前記衛星プロセッサが、前記ホスト乱数を確認するために、前記ホスト変形および前記ホスト乱数を使用する装置。

【請求項 12】 請求項 11 に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数の非可逆的変形から前記ホスト変形を計算する装置。

【請求項 13】 通信ネットワークを通して、取引を確認するための装置であって、

(i) 前記通信ネットワークを通して、第二プロセッサから第二のプロセッサ入力変形を受信し、

(ii) 任意の ゲーム入力を発生し、

(iii) 前記任意の ゲーム入力から第一のプロセッサ入力変形を計算し、

(iv) 前記第一のプロセッサの入力変形を、前記通信ネットワークを通して、第二のプロセッサに送り、

(v) (i) および (iv) ステップの後で、前記通信ネットワークを通して、

前記任意のゲーム入力を前記第二のプロセッサに送り、

(v i) 前記通信ネットワークを通して、前記第二のプロセッサから任意のゲーム入力を受信し、

(v ii) (v i) ステップの後で、前記第二のプロセッサの入力変形を、(v i) ステップで受信した前記任意のゲーム入力と比較するための第一プロセッサと、

(i) 前記通信ネットワークを通して、前記第一のプロセッサから前記第一のプロセッサの入力変形を受信し、

(ii) 第二の任意のゲーム入力を発生し、

(iii) 前記の任意の決定入力から前記第二のプロセッサの入力変形を計算し、

(i v) 前記通信ネットワークを通して、前記の第二のプロセッサの入力変形を前記の第一のプロセッサに送り、

(v) (i) および (v) ステップの後で、前記通信ネットワークを通して、前記の第二の任意のゲーム入力を前記の第一のプロセッサに送り、

(v i) 前記通信ネットワークを通して、前記の第一のプロセッサから前記の任意の決定入力を受信し、

(v ii) (v i) ステップの後で、前記第一のプロセッサの入力変形を、(v i) ステップで受信した前記任意の決定入力と比較するための第二のプロセッサとを備える装置。

【請求項14】 請求項13に記載の装置において、前記第一のプロセッサの入力変形および前記第二のプロセッサの入力変形が、前記決定入力の非可逆的変形に基づくものである装置。

【請求項15】 通信ネットワークを通して、公正なゲーム進行手続を確保するための装置であって、

(i) 通信ネットワークを通して、二つの各衛星プロセッサから任意のゲーム入力を受信し、

(ii) 各衛星プロセッサに対する前記任意のゲーム入力に対応するデータを前記の他の衛星プロセッサに送り、

(iii) 前記の二つのプロセッサからの任意のゲーム入力、および予め定めたゲームの規則を使用して、ゲームの結果を作成し、

(iv) 前記通信ネットワークを通して、前記のゲームの結果を前記衛星プロセッサに供給し、

(v) (iv) ステップの後で、前記通信ネットワークを通して、すべての任意のゲーム入力を各衛星プロセッサに供給するためのホスト・プロセッサと、

(i) 任意のゲーム入力を決定し、

(ii) 前記通信ネットワークを通して、前記の任意のゲーム入力を前記ホスト・プロセッサに供給し、

(iii) 前記通信ネットワークを通して、前記のゲームの結果を前記ホスト・プロセッサから受信し、

(iv) 前記通信ネットワークを通して、前記ホスト・プロセッサから前記のゲームの結果を受信し、

(v) 前記のゲームの結果を記憶し、

(vi) 前記通信ネットワークを通して、前記ホスト・プロセッサから前記の他の衛星プロセッサのゲーム入力を受信し、

(vii) 前記の他の衛星プロセッサのゲーム入力を記憶し、

(viii) (a) 前記の他の衛星プロセッサの任意のゲーム入力と、前記の記憶した任意のゲーム入力と、前記記憶した予め定めたゲームの規則からゲームの結果を発生し、

(b) 前記の発生したゲームの結果を、前記の記憶したゲームの結果と比較することにより、前記ゲーム実行取引を確認するための二つの各衛星プロセッサを備える装置。

【請求項16】 請求項15に記載の装置において、前記ホスト・プロセッサが、さらに、

前記各衛星プロセッサのゲーム入力から発生したデータを受信し、

前記通信ネットワークを通して、前記各衛星プロセッサからの前記発生データを前記の他の衛星プロセッサに転送し、

また、各衛星プロセッサが、さらに、

- (i) 前記ホスト・プロセッサに前記ゲーム入力から発生したデータを供給し、
- (ii) 前記の他の衛星プロセッサからの前記ゲーム入力からの発生データを受信し、
- (iii) 前記の他の衛星プロセッサから前記ゲーム入力を受信した後で、前記ゲーム入力に対応するデータを計算し、前記出力を計算したデータと呼び、
- (iv) (iii) ステップの後で、前記ゲーム入力から計算したデータと、前記ゲーム入力に対応する前記の前に受信したデータとを比較する装置。

【請求項17】 請求項15に記載の装置において、前記決定入力に対応する前記データが、前記決定入力の非可逆的変形から計算される装置。

【請求項18】 請求項15に記載の装置において、前記ホスト・プロセッサが、各衛星プロセッサに対する前記任意の決定入力に対応するデータを計算する装置。

【請求項19】 前記衛星プロセッサが、前記ホスト・プロセッサに乱数を供給し、

前記ホスト・プロセッサが、前記の受信した乱数に基づいて、ゲーム・シードを発生し、

前記衛星プロセッサが、前記ホスト・プロセッサにゲーム入力を供給し、

前記ホスト・プロセッサが、前記ゲーム入力、前記ゲーム・シード、および予め定めたゲームの規則に基づいて、ゲームの結果を発生し、

前記衛星プロセッサが、前記ホスト・プロセッサから、前記ゲーム・シードおよび前記のゲームの結果を受信し、

前記衛星プロセッサが、(i) 前記ゲーム入力、前記ゲーム・シードに対応する前記データ、および予め定めたゲームの規則に基づいて、ゲームの結果を発生し、(ii) 前記の発生したゲームの結果を、前記の受信したゲームの結果と比較することにより、前記取引に不公正な行為がないことを確認し、これらのプロセスにより、通信ネットワークを通して、一つまたはそれ以上のコンピュータに、公正なゲーム進行手続を確保するためのプログラムを記憶するための記憶媒体。

【発明の詳細な説明】**【0001】****【発明の分野】**

本発明は、通信ネットワークを通して公正なゲーム進行手続を確保するための装置および方法に関し、特に、インターネットによるゲーム取引を確認するための装置およびプロセスに関する。

【0002】**【関連技術】**

ゲームおよび賭事は、恐らく、人類最初の発明の中の二つの発明であろう。そしてその後で、すぐに不公正な行為が行われるようになった。それ以来、賭事の魅力的なスリルのために、不公正な行為を行う者と、不公正な行為をしないゲーム参加者とカジノとの間で闘争が行われてきた。この闘争のために、両者の間で、すなわち、公正なカード、公正なダイス、および積み込みデッキと、カジノの胴元、ビデオ・カメラおよびゲーム実行委員会との間で、精巧ないくつかの発明が行われてきた。賭博には簡単に金が手に入るという魅力があり、また飛びきりの「スリル」を味わいたいという誘惑を持っていたために、政界のリーダーおよび宗教界のリーダーが、ゲームを規制し、または禁止してきた。今日、各国の政府は、ゲーム・ビジネスを厳しく規制しているところもあるし、またはゲーム・ビジネスを行っているところもあるが、ゲーム・ビジネスは、何十億ドルという大金が動く娯楽業界であり、数百万の人がそれに参加している。

【0003】

インターネットは、従来からのゲーム技術に対する新しい挑戦であり、新しい機会を提供している。この世界的なネットワークにより、人びとは、自分の町でゲームを行うこともできるし、自分の家にいながら全世界の好きなところでゲームを楽しむことができる。そのため、多くの企業が刺激を受け、政府がそれに対して関心を持つようになった。インターネット上に、もぐりのゲームの亡霊が登場し、不公正な行為および乱用の恐れから、再び、ゲームの禁止を求める声が起こってきた。

【0004】

このような問題を発生させたネットワーク、およびコンピュータ技術は、現在一つの答えを持っている。ゲームに対する不公正な行為の問題、およびネットワークを通してのゲームのプレイのサポートの問題の両方を解決しようとして、今まで、種々の発明が行われてきた。最も代表的な例が、米国特許第5,586,937号である。上記特許およびそれ以前の特許は、コンピュータまたはターミナルとホスト・コンピュータとの間で、ゲーム情報を配布するための手順を供給してきた。これらの特許は、せいぜい、プライバシーを保護し、ホストとプレーヤとの間の取引をある程度制御するだけのものであった。これらの特許の多くは、「公平」について記載しているが、主として賭博場を、ゲーム参加者による不公正な行為やゲーム操作から保護するためのものである。他の現在のネットワーク機密保護および電子商取引技術も、プライバシーの保護とゲームの実行または取引の信頼性に焦点を当てている。ゲーム参加者を、カジノによる不公正な行為から保護するという重要な問題、および自主的な確認という重要な問題は未解決のままである。

【0005】

それ故、新しい方法で、個人を保護し、規制が、現在のコンピュータおよび暗号機能を使用することができるようにするシステムが求められている。カジノは、いかなる方法でも、自分達を騙すことはないという確信をもって、ゲームをするために、ゲーム参加者が、普通のホーム・コンピュータおよびソフトウェアを使用できなければならない。規制を行う側は、カジノおよびゲーム参加者が、不公正な行為をしないでゲームを行ったことを立証するために、不公正な行為の疑いのあるゲームを再現できなければならない。カジノ自身は、ゲーム参加者により騙されていないことを確信できなければならない。

【0006】

【発明の概要】

本発明は、従来の技術に基づくものであるが、カジノまたはゲーム参加者による不公正な行為の問題を解決する。実際、このような解決により、インターネットによるゲームを、従来の認可を受けているカジノに行くよりも、もっと信頼できるものにする。ゲーム参加者は、すべてのランダムなゲーム・イベントを生成

することを助け、ゲームが終了した後で、個々のゲームを再検討するのを助ける。このような行為は、トランプのカードを切り終わり、ゲームが始まる前に、カードによるゲームに参加した者が、「カードをもう一度切る」ことができるのと同じことである。ゲーム終了後、ゲーム参加者は、全部のカードの「分配」を再現するために、カジノの「カードを切った行為」を再現することができる。

【0007】

もう一つの特徴は、秘密で同時の決定をサポートすることができることである。この最も簡単な使用例は、子供の遊びである、「グウ、チョキ、パー」である。このゲームの場合、ゲーム参加者は、自分が「グウ、チョキ、パー」の中のどれを選ぶかを同時に決める。ゲーム参加者が、他の参加者が何を行なったかを見た後の最後の瞬間に、自分の決定を変えた場合に問題が起こる。新しいシステムを使用すれば、ゲーム参加者は、三種類の選択を行い、要求されるまで、選択それ自身を知らせないで、自分が選択を行なったことを知らせることができる。（それと知らせないでチョキを選択し、チョキを選択したことを否定することができる。）

【0008】

本発明は、ゲーム参加者のパソコン上のソフトウェアと、通信ネットワークにより接続しているカジノのホスト・コンピュータとを組み合わせ、これら技術を実行する。ゲーム参加者のパソコンおよびホスト・コンピュータは、本明細書に記載するプロトコルにより、配布されたゲーム情報を通信する。これらの技術は、任意の通信ソフトウェア上、または特定のゲーム用のソフトウェアの下に位置する、ソフトウェアの別々の層で実行される。そのため、ウェブ・サーバに接続しているウェブ・ブラウザと同じ方法で、ゲーム参加者とカジノとの間で通信することができるように、ワールド・ワイド・ウェブに非常によく似た「ミドルウェア」層を供給する。

【0009】

本発明を使用すれば、インターネットによるゲームは、単に技術的に実行可能になるばかりでなく、政治的にも可能になる。ゲーム参加者は、オンライン・カジノを自信をもって信用し、政府は、オンライン・カジノを規制することができる。

るようになるだろう。新しいゲームの可能性が開け、本明細書に記載するミドルウェアおよびプロトコル上に全く新しいゲームを形成することができる。経済的可能性、社会的可能性および娯楽としての可能性は、インターネット自身のように、予想できないし、無限なものになるかもしれない。

【0010】

第一の観点から見た場合、本発明は、通信ネットワークを通してのゲーム取引が不公正な行為のないことを確認するための装置および方法であり、それにより、ホスト・プロセッサが、ホスト乱数を生成し、通信ネットワークにより、衛星プロセッサから乱数を受信し、その乱数に基づいてゲーム・シードを発生する構造とステップとを含む。ホスト・コンピュータは、また、衛星プロセッサからゲーム入力を受信し、上記ゲーム入力、ゲーム・シード、および予め定めた組のゲームの規則に基づいて、ゲームの結果を発生する。衛星プロセッサは、通信ネットワークを通してホスト・プロセッサに、乱数とゲーム入力を供給し、ホスト・プロセッサから対応するデータおよびゲームの結果を受信する。その後で、衛星プロセッサは、(i) ゲーム入力、ゲーム・シードに対応するデータ、および予め定めたゲームの規則に基づいて、ゲームの結果を発生し、(ii) 発生したゲームの結果を、受信したゲームの結果と比較することにより、取引に不公正な行為がないことを確認する。

【0011】

第二の観点から見た場合、本発明は、通信ネットワークを通しての、ゲーム取引が不公正な行為のないことを確認するための装置および方法であって、構造体およびステップを含み、それにより、ホスト・プロセッサは、下記のことを行う。

(i) ホスト乱数の決定；

(ii) 通信ネットワークを通しての、衛星プロセッサへのホスト乱数の非可逆的変形の供給；

(iii) 通信ネットワークを通しての、衛星プロセッサからの衛星乱数を受信；

(iv) ホスト乱数および衛星乱数からのゲーム・シードの発生；

(v) 衛星プロセスからの、任意のゲームの決定の入力の受信；

(v i) ホスト乱数、衛星乱数、ゲーム・シード、任意のゲームの決定の入力、および予め定めたゲーム規則の記憶；

(v ii) ゲーム・シードからの、ランダム・イベントの発生；

(v iii) ゲームの決定の入力、ランダム・イベント、および予め定めたゲームの規則を使用するゲームの結果の発生；

(i x) 通信ネットワークを通しての、衛星プロセッサへのゲームの結果の供給；

(x) 通信ネットワークを通しての、衛星プロセッサへのホスト乱数およびゲーム・シードの供給；

【0012】

衛星プロセッサは、下記のことを行う。

(i) 通信ネットワークを通しての、ホスト・プロセッサからのホスト乱数の非可逆的変形の受信；

(ii) 衛星乱数の決定；

(iii) 通信ネットワークを通しての、ホスト・プロセッサへの衛星乱数の供給；

(i v) ホスト・プロセッサへの任意のゲームの決定の入力の供給；

(v) ホスト乱数の非可逆的変形、予め定めたゲームの規則、およびゲーム決定入力の記憶；

(v i) 通信ネットワークを通しての、ホスト・プロセッサからのゲームの結果の受信；

(v ii) ホスト・プロセッサからのホスト乱数およびゲーム・シードの受信；

(v iii) (a) 受信したホスト乱数の非可逆的変形の発生、(b) 発生した変形と、前に記憶したホスト乱数の非可逆的変形との比較、(c) ホスト乱数および衛星乱数からの、ゲーム・シードの再構成、(d) 記憶したゲームの決定の入力、および記憶した予め定めたゲームの規則を使用するゲームの発生；(e) 発生したゲームの結果と、受信したゲームの結果との比較による、ゲームの確認。

【0013】

複数の衛星プロセッサが設置されている場合には、各衛星プロセッサは、すべての衛星プロセッサからの衛星乱数を使用して、ゲーム・シードを再構成する。

【0014】

【好適な実施形態の詳細な説明】

1.

本出願は、すべてのゲーム・イベントの場合に、「トランプを切る」ことができ、ゲームを行い、ゲーム終了後に、すべてのゲーム・イベントを再現することができるようにするための、ゲーム参加者のコンピュータと、カジノのコンピュータとの間のプロトコルに関する。種々の形の不公正な行為を排除し、すべての疑わしいゲームを再検討することができるようにすることにより、このシステムは、インターネットによるゲームを安全にし、その機密を保護して、多くの疑心暗鬼の政府、慎重な消費者を通して用心深いビジネスの反対意見を有意に軽減する。この技術は、また、インターネットおよび他のネットワークによる、他のタイプの取引にも適用することができ、カジノで行われるゲームおよびゲーム活動を他の方法で実行することができる。

【0015】

本明細書は、インターネット・ゲームに使用される、立証可能な不公正な行為のない分散型取引処理システムについて記載する。クライアントは、自動化ホスト・カジノを使用して、ゲームを行っているゲーム参加者である。ゲーム参加者のコンピュータ上の、ソフトウェアにより実行される中心となる取引システムは、一意のゲーム・プロトコルにより、ホストであるカジノ・コンピュータと通信する。（ブラックジャック、クラップス、または新しいゲームのための）ゲーム・アプリケーションの一意の部分は、この不公正な行為のないゲーム・システムを実行するために、この共通のミドルウェア層の上に位置する。

【0016】

2. 実施形態

分散型ゲーム・システムの全体の機能アーキテクチャは、一つまたはそれ以上のゲーム参加者とカジノを備える（図1）。この図に示すように、ゲーム参加者の間の取引を含むすべての取引は、ホスト・カジノ・コンピュータを通して

行われる。別の観点から機能アーキテクチャを見ると、このアーキテクチャは、クライアントである、ゲーム参加者のゲーム・アプリケーション、サーバである、ホスト・ゲーム・アプリケーション、およびネットワーク・ゲーム実行プロトコルを含む分散型ゲーム実行システム・「ミドルウェア」アプリケーションからなる（図2）。

【0017】

このアーキテクチャは、三つの手段の中の一つ、すなわち、ローカル・エリア・ネットワークを通しての直接接続、モデムを通しての電話リンク、またはインターネットのようなワイド・エリア・ネットワーク接続により、ゲーム参加者のコンピュータと通信することができるホスト・コンピュータにより実行することができる（図3）。

【0018】

ホスト・カジノ・システムは、一つまたはそれ以上のコンピュータ上で実行することができる多数のアプリケーションを含む。すなわち、ウェブ・サーバのようなフロント・エンド、会計システム、ゲーム確認システム、登録システム、監査システム、顧客サービス・システム、およびゲーム・プロトコルをサポートし、複数のゲーム・アプリケーション・セッションを制御するゲーム・マネージャである（図4）。これは、ディスプレイ、コンピュータ・プロセッサ、およびオペレーティング・システム、キーボードのような入力デバイス、ハードディスクのような大量記憶システム、および長期間記憶するためのアーカイブを含むプラットフォーム上で実行される（図5）。

【0019】

ゲーム参加者システムは、ゲーム・プロトコル・パッケージ、ゲーム確認アプリケーション、および一つまたはそれ以上のゲーム・アプリケーションを含む（図6）。ゲーム参加者のプラットフォームは、ディスプレイおよびオペレーティング・システム、キーボードのような入力デバイス、オペレーティング・システムを含むコンピュータ・プロセッサ、ハードディスクのような大量記憶システム、および通信デバイスを備える（図7）。

【0020】

本発明は四つの主要なプロセスを実行する。すなわち、ゲーム参加者の登録、ゲームの設定、ゲームの実行、およびゲームの確認である。二つのサポーティング・プロセス、すなわち、機密保護ホスト・ゲーム参加者間の通信、およびホスト・ゲーム参加者間の取引が行われるが、それについては、以下に詳細に説明する。これらプロセスは相互に、またコア・ゲーム・プロセスと入れ子状態になっている。コア・ゲーム・プロセスは、取引プロセスで実行され、取引プロセスは、通信プロセスで実行される（図8）。これら六つのプロセス全体のための、ゲーム参加者とホスト・カジノ間の情報の交換は、ネットワーク・ゲーム実行取引処理プロトコルを構成する。実行の可能性のある他のプロセスは、ゲーム実行とホストとの間の金融取引に関する会計ためのプロセス、ゲーム参加者へ、ゲームおよびミドルウェア・プロトコル・ソフトウェアを供給するためのソフトウェアの配布、および顧客の問題を解決するための顧客サービスである。

【0021】

ゲーム参加者の登録は、ゲームができるように、口座を開設するためにゲーム参加者が、ホスト・カジノとコンタクトするプロセスである（2. 1節）。ゲーム参加者は、また条件および、ゲーム参加者が、金を賭け、ゲームを行い、預金をし、元手を回収するためのカジノの規則と、コンピュータでの脱落した、切断された、または失われたネットワーク接続およびそのほかの問題、およびカジノで生じないネットワーク・ゲームの両方を確実に理解するために必要な同意を設定するために、ゲーム参加者は、また、サインをし、カジノとコンタクトする。

【0022】

ゲームの設定は、登録したゲーム参加者が、ホスト・カジノに接続し、自分が行うゲームを選択するプロセスである（2. 2節）。このプロセスは、また、ゲームの初期パラメータの交換および確立を含む。このプロセスは、さらに、ポーカーのような複数のゲーム参加者が参加する、ゲームの設定およびそれへの入力を含む。

【0023】

ゲームの実行は、ゲーム設定プロセスを終了した、登録済みゲーム参加者が、オンラインでゲームを行うプロセスである（2. 3節）。このプロセスは、ホス

ト・カジノによるゲーム参加者の決定の処理、およびゲーム参加者へのホスト・カジノによるゲーム・イベントの通信を含む。このプロセスは、また、ゲームの規則を確実に守らせ、そうでない場合には、適当な処置をとるためのある種の増分確認を含む。

【0024】

ゲームの確認は、不公正な行為が行われなかったことを確認するために、ゲーム・イベントおよびパラメータを再現するプロセスである（2. 4節）。このプロセスは、ゲーム参加者なら誰でも、また、カジノまたは独立の監査人または規制者により行うことができる。ゲームを行っている間に生成されたランダム・シーケンスは、確定的ランダム化プロセスおよび協力ランダム／シード発生プロセスにより再現される（3. 4. 4節）。また、このプロセス中に、ゲームからのすべての秘密が明らかにされ、確認される。これら秘密により、すべての観察されたゲーム・イベントと一緒に、不公正な行為が行われなかったこと、および不公正な行為が行われた場合には、どんな不公正な行為が行われたのか、また誰が不公正な行為を行ったのかを確認するために、ゲームが行われている間のすべての活動を完全に再現することができる。ゲーム確認プロセスにより、立証可能な不公正な行為を防止できる。

【0025】

ホストとゲーム参加者との間の取引プロセスにより、ゲーム参加者とホストであるカジノが、すべての情報（特に、ゲーム・プロセスからの情報）が、正しく受信されているという確信をもつことができる（2. 5節参照）。この取引プロセスは、さらに、米国署名規格のような、デジタル署名機能を使用することにより、データの信頼できる交換のための周知の「ハンドシェイク」プロトコルに基づいている（3. 4. 3節）。この機能により、ゲーム・プロセス情報が、正確であり、ゲーム参加者またはホストであるカジノにより発生したものであるという、非常に強い確信を与えることができる。その確信および「非拒絶」機能を供給するために、何か他の機構または同意が代わりに使用されている場合には、このプロセスを省略することができる。図面に、ホストーゲーム参加者間の、取引プロセスにより保護する必要があるプロセス・ステップをハッキリと示す

。

【0026】

機密保護ホストーゲーム参加者間の通信は、ゲーム参加者が、ホストであるカジノとの接続を設定するプロセスである。このプロセスにより、その通信のためのプライバシーが保護され、このプロセスの間のゲーム参加者の身元の秘密が守られる。ゲーム参加者は、自分が特定のカジノと通信していることを知っているし、また、カジノは、自分が特定のゲーム参加者と通信していることを知っている（2. 6 節）。このプロセスは、ホストであるカジノと、個々のゲーム参加者との間のすべての通信に対して使用される。ゲーム参加者が、ゲーム参加者間で通信を行うことができるゲームに参加している場合には、ホストであるカジノは、ゲーム参加者間のこれら通信を転送するために、通信プロセスを使用する。ゲーム参加者間で直接通信は行われな（図1）。このサービスを供給するために使用することができる、機密保護ソケット層プロトコルのような、市販で周知の製品が販売されている。カジノまたは他の場所またはプライバシーの保護が問題にならない環境で、通信を行う場合にも、このプロセスの身元確認機能が依然として必要である。図面においては、機密保護ホストーゲーム参加者間の通信プロセスにより保護する必要がある、プロセス・ステップは強調してある。

【0027】

この発明が機能する理論を供給するいくつかの技術およびコンセプトがある。これら技術およびコンセプトについては、以下の詳細な説明のところで、必要に応じて説明し、本明細書の個々の節で説明する（3 節）。主題は下記の通りである。

【0028】

ゲーム取引処理システム・アーキテクチャ — 大部分のゲーム取引処理システムを、取引プロセス活動の処理の自動化を容易にする、一組の素子に分解するための方法（3. 1 節）。

【0029】

信頼性レフリー・モデル — ゲームのような規則をベースとするシステムを調停し、ゲーム中またはゲーム終了後で、ゲーム中に不公正な行為が行われな

ったことを確認するためのアプローチ（3．2節）。

【0030】

不公正な行為のないモデル — 不公正な行為を確実に防止するための、システムの強さおよび制限の説明（3．3節）。

【0031】

ランダム化装置 — ダイスまたはカード類似の予測できない結果を発生するための、コンピュータ・デバイスまたはアルゴリズムおよび手段（3．4．1節）。

【0032】

非可逆的変形 — その機能の出力が分かっている場合でも、入力データを再現するのが困難であるという特徴を持つ数学的機能（簡単な例は電話帳である。所与の名前の電話番号を見つけることは簡単であるが、処理されるすべてのものが電話番号であり、電話帳のコピーである場合には、その名前を見つけるのは非常に難しい）（3．4．2節）。

【0033】

署名およびハッシュ機能 — データが操作されていないこと、およびそのデータが、ある特定の個人により、生成されたものであるという確信を与えるための方法（3．4．3節）

【0034】

協力シード／ランダム発生 — ゲーム参加者が、「カード」の結果として得られるランダムなシーケンスを、ゲーム終了後に、再計算することができるようにする一方で、賭博場と一緒に電子的に「カードを切る」ことができるようにする、乱数を生成するための方法（3．4．4節）。

【0035】

また、引用によって本明細書の記載に援用した、1995年発行のブルース・シュナイダ著の「応用暗号術」第二版を参照されたい。

【0036】

本明細書全体にわたって使用されるもう一つの特徴はログである。ログは、必要なデータを記録し、保存するために、シーケンシャルな情報を記憶するための

手段である。個人の日記または小切手帳は、データ・ログの例である。

【0037】

本発明の全体の効用は、個人がカジノでゲームを行うことにし、カジノに登録し、自分が行うゲームを選択し、ゲームを行い、不公正な行為が行われなかったことを知るために、ゲームをチェックするプロセスを考えれば、最もよく理解することができる（図9）。

【0038】

下記のシーケンスは、ゲーム参加者がすでに必要なコンピュータ、ソフトウェア、およびホストであるカジノに接続するための、他の基本的材料を所有していると仮定した場合のものである。

【0039】

2. 1 ゲーム参加者の登録

ゲーム参加者の登録とは、ある個人が、ホストであるカジノでゲームを行うことを決めた場合に、その人が最初に行うプロセスである（図11）。表1は、このプロセスのために使用するデータを示す。

表1

ゲーム参加者の登録を示すデータグラムの内容

【表1】

フィールド名	説明	データ・タイプ
ヘッダ・データ		
ギャンブル参加者ID	ギャンブル参加者の一意の識別子	整数
賭博場ID	賭博場の一意の識別子	整数
登録ペイロード		
登録内容	登録ステップ情報のために、すべてを送るために使用する登録図	データ構造
登録例外情報	プロセスの正しい実行のすべての例外を他の関係者に通知するために使用するエラー・コード	データ構造

【0040】

ゲーム参加者の登録開始

1. ゲーム参加者は、ホスト・カジノの登録アプリケーションにコンタクトするために自分のパソコンを使用する。

2. 次に、ホストで・カジノ登録アプリケーションは、ゲーム参加者のパソコンに、ゲームを行うための約定および条件を要約した情報を送る。この情報は、金の賭け方、ゲームの実行、元手の預金と回収、および脱落、中断または失われたネットワーク接続および他の問題を解決するための手順を含む。ホストであるカジノは、ゲーム参加者のパソコンに、最初の取引きシーケンス番号を送る（2.5節）。

3. ゲーム参加者が条件を受け入れることを決めた場合には、ゲーム参加者は、ホストであるカジノに通知するために、自分のパソコンを使用する。

ゲーム参加者の口座の開設

4. その後で、ホストであるカジノは、ゲーム参加者のパソコンに、情報および金融データを識別するようにプロンプトする。金融データは、口座番号、振込または預金金額、およびゲームで勝った金の支払いおよび受領のための他の方法のような情報を含むことができる。

5. ゲーム参加者は、自分の名前、およびホストであるカジノへの他の必要な情報を送るために、自分のパソコンを使用することができる。

6. ホストであるカジノは、識別情報および金融情報を処理する。

7. ゲーム参加者が送った情報について、法律的な問題、金融上の問題または他の問題がある場合には、ホストであるカジノは、ゲーム参加者が修正することができるように、上記問題をゲーム参加者のパソコンに送り、できれば、（ステップ5に戻る。）

8. 何も問題がない場合には、ホストであるカジノは、その口座のデータベースに、上記情報を記憶する。

ゲーム参加者の一意の識別情報の配布

9. ホストであるカジノは、パスワード、機密保護のホストーゲーム参加者間の通信プロトコル用のキー、およびデジタル署名機能用のキーのような任意の一意の識別情報を発生する。

10. ホストであるカジノは、この一意の識別情報をゲーム参加者のパソコンに送る。ホストであるカジノは、また、ゲーム参加者のパソコンが、それがホストであるカジノとの通信であることを識別することができるような情報を送る。

11. ゲーム参加者のパソコンは、一意の識別情報を記憶する。

正式な契約の作成

12. ホストであるカジノは、パソコンを通して、ゲーム参加者に、カジノを使用するためのすべての詳細な約定および条件を含む、正式な契約を送る。この契約は、法的および規制要件により、通常郵便で送り、処理しなければならない場合がある。

13. ゲーム参加者が、契約に同意しない場合には、ゲーム参加者は、ホストであるカジノに、その旨のメッセージを送るために自分パソコンを使用する。その場合、すでに記憶したすべての情報は削除され、この人の口座を開設されない。

14. ゲーム参加者が契約に同意する場合には、ゲーム参加者は、その旨のメッセージをパソコンに送るために、自分のパソコンを使用する。この場合には、口座が開かれ、記憶され、ゲーム参加者は、ゲームの設定に進むことができる。

【0041】

2. 2 ゲームの設定

ゲームの設定とは、登録したゲーム参加者が、ホストであるカジノに接続し、自分がプレイするゲームを選択し、そのゲームを初期化するプロセスである（図12）。表2は、このプロセスのためのデータ要件を示す。

表2

ゲーム設定データグラムの内容

【表2】

フィールド名	説明	データ・タイプ
ヘッダ		
ギャンブル参加者ID	ギャンブル参加者の一意の識別子	整数
他のギャンブル参加者IDの組	そのギャンブルの、すべてのギャンブル参加者の一意の識別子のリスト	整数の組
賭博場ID	ホスト・カジノの一意の識別子	整数
ギャンブルの規則識別子	ギャンブルの普通名	賭博場が認識したプレイすることができるギャンブルの一覧表
ギャンブル名	プレイ中のギャンブルのタイプの一意の識別子	賭博場が認識したプレイすることができるギャンブルの一覧表
ギャンブルID	プレイ中の特定のギャンブルの一意の識別子	整数
ギャンブルの活動シーケンス番号	特定のギャンブルのイベントまたは決定の一意の数。賭博場だけが確立。取引が承認されるまで指定されない。	整数
設定活動のタイプ	これがギャンブル確立であるのか、協力乱数発生活動であるのかどうかを識別する数値	一覧表（確立、乱数発生）
ギャンブル・プロトコル設定ペイロード		
ギャンブル・プロトコル設定例外情報	すべてのギャンブル参加者、および賭博場への、ギャンブル・プロトコルの、正しい実行へのすべての例外の通知	データ構造 ⁽¹⁾

(1) ゲーム・プロトコル、および使用した任意の規格または市販技術（オペレーティング・システム、エラー処理ライブラリ等）の一意の構造

表2（続き）

ゲーム設定データグラムの内容

下記の追加情報は、協力乱数発生だけに使用される。

【表3】

フィールド名	説明	データ・タイプ
ギャンブル参加者のランダムなシード	協力ランダム発生の際に使用するための、ホストであるカジノへ、ギャンブル参加者が供給する乱数	賭博場とのギャンブル参加者の通信のためだけに指定される2進シーケンス
ギャンブル参加者のランダムなシードの組	協力ランダム発生の際に使用するための、ギャンブル参加者IDを持つ、一組のギャンブル参加者が供給する乱数を識別する一組のペアの形をしているデータ（ギャンブル参加者ID、ランダム・シード）。このデータは、設定段階中にホスト・カジノにより使用され、確認段階まで他のギャンブル参加者により記憶される。	整数および2進シーケンスの一組の順番に並べたペア
賭博場のランダムなシード	協力ランダム発生の際に使用するための、賭博場が発生した乱数。ホスト・カジノは、賭博場ランダム・キーを記憶する。ギャンブル確認プロセスまで、ギャンブル参加者に供給されない。	2進シーケンス
賭博場のランダムなシードの非可逆的変形	協力・ランダム発生のために、ホスト・カジノが使用する、ランダムなシードの非可逆的変形。これは、ギャンブル確認プロセス中にギャンブル参加者が使用するように、この段階中にギャンブル参加者に供給される。この情報は、個々のギャンブル参加者、およびホスト・カジノにより記憶される。	2進シーケンス
ギャンブル・シード	ギャンブル中に使用するために、確定的なランダムなデータを生成するために実際に使用される協力ランダム／シード発生プロセスにより生成されたシード。ギャンブルのプレイ中にホスト・カジノにより記憶され、使用される。このシードは、ギャンブル確認プロセスまで、ギャンブル参加者に供給されない。	2進シーケンス

【0042】

ゲーム設定開始

1. ゲーム参加者は、ホスト・カジノのところで、ゲームをプレイすることを決める。
2. ゲーム参加者は、ホスト・カジノに接続するために、自分のパソコンを使用する。

ゲーム参加者の口座確認

3. ホスト・カジノは、自分のパソコンを通して、自分の口座情報およびある種の識別情報をプロンプトする。これが、ホスト・カジノとのセッションの始まりである場合には、ホスト・カジノは、ゲーム参加者のパソコンに、初期取引シ

ーケンス番号を知らせる（2.5節）。

4. ゲーム参加者は、ホスト・カジノに、自分の口座情報および識別情報を送るために、自分のパスワードを使用する。ゲーム参加者のパソコンは、いくつかまたはすべての口座情報、および識別情報をすでに記憶している場合があり、自分のパソコンがホスト・カジノに接続した場合、またはホスト・カジノによりプロンプトされた場合、この情報を自動的に送ることができる。

5. ホスト・カジノは、送られてきた口座情報および識別情報をその会計データベースと照合して確認する。

6. 確認できなかった場合には、ホスト・カジノは、自分のパソコンを通して、自分の口座情報および識別情報を再入力する（ステップ3へ行く）ように、ゲーム参加者にプロンプトすることもできるし、またはホスト・カジノは、接続を終了することもできる。

ゲーム参加者のゲームの選択

7. 確認できた場合には、ホスト・カジノは、自分パソコンを通して、ゲーム参加者に、ゲームを選択するためのオプションを含む、入手することができるオプションをゲーム参加者にプロンプトする。

8. その後で、ゲーム参加者のパソコンは、自分の決定をホスト・カジノに知らせる。

9. ゲーム参加者がゲームのプレイ以外の何かをしようと決めた場合には、ホスト・カジノは、これらオプションをサービスし、再び、自分のパソコンを通して、ゲーム参加者にプロンプトする（ステップ7へ行く）。

10. ゲーム参加者が、ゲームをプレイすると決めた場合には、ホスト・カジノは、利用できるゲームのリストをゲーム参加者のパソコンに知らせる。プレイする特定のゲームの他に、この時点で選択することができる基準の中のあるものは、複数のプレーヤが参加するゲームの開始または結合を含むことができる。これは、ゲーム名およびゲームの規則識別子の両方を含む。ゲーム名は、ブラックジャック、クラップスおよびポーカーを含むことができ、一方、ゲームの規則識別子は、ブラックジャックに使用するデッキの数、クラップスの場合に使用することができる賭けの種類、プレイ中のポーカーの種類（または、プレイできるゲ

ームの種類)、およびゲーム参加者相互間の動作が許されるかどうかを含むことができる。ゲーム参加者のパソコンは、ゲーム参加者とホストが必ず同じ規則を使用するように、ゲーム名とゲームの規則識別子の両方を送る。ゲーム参加者のパソコンのゲームの規則識別子が、ホスト・カジノが送ったゲームの規則識別子と異なる場合には、ゲーム設定例外処理に行く(ステップ37)。

11. ゲーム参加者は、自分の決定を賭博場に送るために、自分のパソコンを使用する。

カジノ・ゲームの設定

12. ホスト・カジノは、選択したゲームのすべての初期属性を生成する。この生成は、表2に示す属性を含む。この中で、最もよく知られているのは、ゲームIDおよびゲーム・シーケンス番号である。追加の属性としては、ゲーム参加者のパソコンおよびホスト・カジノが、必ず同じゲームの規則を使用するようにするために使用される、一意のゲームの規則識別子がある。

13. ホスト・カジノは、ゲームの確認をサポートし、ゲームの状態を追跡するために、ゲームが行われている間使用するために、賭博場ゲーム・ログ内にこれら属性を記憶する。ホスト・カジノは、行われた各ゲーム毎に、賭博場ゲーム・ログを生成する。

14. ホスト・カジノは、ゲーム参加者のゲームのプレイをサポートすることができるように、選択したゲーム・アプリケーションのセッションをロード、または作動する。

15. ゲーム参加者が選択したゲームが、ダイスまたはカードのようなランダムなイベントを使用する場合には、ホスト・カジノは、協力ランダム／シード発生プロセスを実行する(ステップ20参照)。

16. ホスト・カジノは、パソコンを通して、ゲームの属性をゲーム参加者に知らせる。

ゲーム参加者のゲームの設定

17. ゲーム参加者のパソコンは、最初のゲーム状態を設定するために、ホスト・カジノから送られてきたパラメータを使用する。ゲーム参加者のパソコンは、ゲームの状態を追跡する目的で、ゲームが行われている間使用するために、これ

ら属性を使用する。ゲーム参加者のパソコンは、ゲームを楽に楽しんでプレイすることができるように、視覚的情報、音声による情報およびその他の情報を供給する、ゲーム環境をロードすることができる。ゲーム参加者のパソコンは、また、ゲームの規則識別子が、ゲームの規則のローカル・コピーに対して同じものであることを確認する。

18. ゲーム参加者のパソコンは、ゲームの確認中に後で使用するために、初期パラメータをゲーム参加者のゲーム・ログ内に記憶する。

19. ホスト・カジノおよびゲーム参加者は、ゲーム・プレイ・プロセスに入る。

協力ゲーム・シードの発生

20. ホスト・カジノは、賭博場ランダム・シードと呼ばれる、内部乱数値を発生することにより、協力ランダム／シード発生プロセスを開始する。このプロセスは、真のランダム化装置またはローカルな確定的ランダム化プロセスを使用して行われる。

21. ホスト・カジノは、賭博場ゲーム・ログ内に賭博場ランダム・シードを記憶する。

22. ホスト・カジノは、自分が発生した賭博場ランダム・シードを取り上げ、予め定めた非可逆的変形機能を使用して、それを、賭博場ランダム・シードの非可逆的変形と呼ばれる、非可逆的に変形したものを生成する。

23. ホスト・カジノは、賭博場ランダム・シードの非可逆的変形を賭博場ゲーム・ログ内に記憶する。

24. ホスト・カジノは、賭博場ランダム・シードの非可逆的変形をゲーム参加者に知らせる。

25. 各ゲーム参加者のパソコンは、賭博場ランダム・シードの非可逆的変形を自分の各ゲーム参加者のゲーム・ログ内に記憶する。

26. 各ゲーム参加者のパソコンは、ゲーム参加者のランダム・シードと呼ばれる内部乱数値を発生することにより、協力ゲーム・シード発生プロセスをスタートする。このプロセスのスタートは、真のランダムマイザ、またはローカルな確定的ランダム化プロセスを使用して行われる。このことは、別々に行うこともでき

るし、ホスト・カジノがそのランダム・シードを発生するときに、同時に行うこともできることに留意されたい。ゲーム参加者のパソコンは、自動的に、またはゲーム参加者の介入により、協力ゲーム・シード発生プロセスの、その一部を実行することができる。

27. 各ゲーム参加者のパソコンは、自分の各ゲーム参加者のゲーム・ログ内に個々のゲーム参加者のランダム・シードを記憶する。

28. 賭博場ランダム・シードの非可逆的変形を受信した後で、各ゲーム参加者のパソコンは、ホスト・カジノに、自分のゲーム参加者のランダム・シードを知らせる。

29. ホスト・カジノは、賭博場ゲーム・ログ内に各ゲーム参加者のランダム・シードを記憶する。

30. ホスト・カジノは、各ゲーム参加者のパソコンに、ゲーム参加者のランダム・シードを知らせる。

31. 各ゲーム参加者のパソコンは、自分が受信する他のゲーム参加者のランダム・シードのすべてを自分のゲーム参加者のゲーム・ログ内に記憶する。

32. ホスト・カジノは、ゲーム・シードを発生するために、それ自身の賭博場ランダム・シードと一緒に、ゲーム参加者のランダム・シードのすべての組を使用する（3.4.4節参照）。このシードは、ゲーム・プレイ・プロセス中に、以降のランダム・イベントを生成するために使用される。

33. ホスト・カジノは、賭博場ゲーム・ログ内にゲーム・シードを記憶する。

34. ホスト・カジノは、ゲーム・シードの非可逆的変形と呼ばれる、ゲーム・シードの非可逆的変形を計算する。

35. ホスト・カジノは、各ゲーム参加者のパソコンに、ゲーム・シードの非可逆的変形を送る。

36. 各ゲーム参加者のパソコンは、自分のゲーム参加者のゲーム・ログ内にゲーム・シードの非可逆的変形を記憶する（ステップ16へ行く）。

ゲーム設定例外処理

37. ホスト・カジノのパソコン、またはゲーム参加者のパソコンは、そのゲームの他の参加者に、ゲームの設定プロセス中に発生するすべての障害を通知する

。これらの障害は、適当なゲーム・ログおよび例外ログ内にログされる。障害が起こると、ゲームの設定プロセスを再スタートさせ、ある既知の状態にゲームの設定プロセスを回復させるために、またはプロセスおよびゲーム・セッションを終了させるために、処理が行われる。この処理は、ゲーム参加者がホスト・カジノに登録した時に、自分が同意したゲームの規則および正式契約により決まる。

【0043】

2.3 ゲームのプレイ

ゲームのプレイとは、ゲーム参加者、賭博場およびゲーム決定、補足シード発生、イベント、および賭けの通信により、実際にゲームを行えるようにするプロセスである（図13）。表3は、このプロセスのデータ要件を示す。

表3

ゲーム・プレイ・データグラムの内容

【表4】

フィールド名	説明	データ・タイプ
ヘッダ		
ギャンブル参加者ID	ギャンブル参加者の一意の識別子	整数
他のギャンブル参加者IDの組	ギャンブル中の、すべてのギャンブル参加者の一意の識別子のリスト	整数の組
賭博場ID	賭博場の一意の識別子	整数
ギャンブルの規則識別子	ギャンブルの通常の名前	賭博場が認識したプレイできるギャンブルの一覧表
ギャンブル活動シーケンス番号	特定のギャンブル内のイベント、または決定の一意の番号。賭博場だけにより設定。処理が承認されるまで指定されない。	整数
プレイ活動のタイプ	イベントか、シード発生か、決定か、公開であるのかを示す識別子	(イベント、シード、決定、公開の) 一覧表
プレイの活動ソースID	活動の作成者のID、ギャンブル参加者、または賭博場のID	整数
プレイ活動の秘匿	活動が秘密なものか、公開のものかを示す識別子	(秘密、公開の) 一覧表
プレイの活動乱数	活動がランダムに発生するものか、そうでないかを示す識別子	ブール
ギャンブル・プレイ・プロトコル・ペイロード		
ギャンブル参加者のランダム・シード	協力ランダム発生の際に使用するために、ギャンブル参加者が供給する乱数	賭博場とギャンブル参加者との通信のためだけに指定される、2進シーケンス
ギャンブル参加者のランダム・シードの組	協力ランダム発生の際に使用するための、ギャンブル参加者IDを持つ一組のギャンブル参加者が供給した、乱数を識別する一組のペアの形をしたデータ (ギャンブル参加者ID、ランダム・シード)	整数および2進シーケンスの順番に並べたペアの組
プレイ活動の内容	イベント、決定または公開活動の内容	データ構造 ⁽¹⁾
プレイ活動の内容の非可逆的変形	イベント、決定、公開または賭博活動の内容の非可逆的変形	データ構造
ギャンブル・プロトコル・プレイ例外情報	すべてのギャンブル参加者および賭博場への、ギャンブル・プロトコルの正しい実行のすべての例外の通知	データ構造 ⁽²⁾

(1) すべてのサポート・パラメータを含むための、ゲーム参加者の決定に一意なデータ構造。内容例の説明参照。

(2) ゲーム実行環境および選択した通信プロトコルに一意なデータ構造。

【0044】

ホスト・カジノは、すべてのゲーム参加者の活動、およびホスト・カジノの活動 (ゲーム・イベント、ゲーム参加者の決定、および例外) をログする。ゲーム参加者は、自分のパソコン上で、ゲームが行われている間に見るすべての活動を

ログするかどうかを自由に決めることができる。最も普通に行われるのは、ゲーム参加者が、自分のパソコン上でのすべての活動をログすることである。ゲーム・プレイ・プロセスの全体の流れは、一連のゲーム・イベントおよびゲーム参加者の決定である。このプロセスは、ホスト・カジノがゲーム・イベントを生成し、そのゲーム・イベントまたはゲーム状態の結果として起こる変化をゲーム参加者に通知した場合にスタートする。ポーカーの際のゲーム・イベントは、カードの内容を見るゲーム参加者Xを除くすべてのゲーム参加者に、「ゲーム参加者Xにカードを伏せて配った」である。ゲームの状態は、すべてのカードが配られ、誰がそれらカードを持っているか、だれがその内容を見ることができるかという、完全な画である。その後で、ゲーム参加者は、決定を応答し、それをホスト・カジノに返送する。このシーケンスは、ゲームが終わるまで継続して行われる。ゲーム・イベントの生成

【0045】

1. ホスト・カジノは、ゲーム・イベントを生成するために、現在のゲーム状態、ゲームの規則、および一人または複数のゲーム参加者の決定をチェックする。二つのタイプのゲーム・イベントがある。すなわち、ランダムなイベントと確定的イベントである。ランダム・イベントへ、ゲーム参加者へカードを配ること、ダイスを転がすことのような行為を含み、一方、確定的イベントは、ボード上でものを移動したり、または賭金を置くような行為を含む。

ランダムなゲーム・イベントの処理

2. ゲーム・イベントが、ランダムなゲーム・イベントである場合には、ホスト・カジノは、ランダム・イベント・シーケンス番号を検索する。ゲーム・イベントが第一のゲーム・イベントである場合には、その数値は初期値に設定される。ダイスの転がり、ゲーム参加者に配られた一枚のカードは、ランダム・ゲーム・イベントの一例である。

3. ホスト・カジノは、ランダム・ゲーム・イベントを生成するために、ゲーム・シードおよび検索したランダム・イベント・シーケンス番号（3. 4. 1節参照）を使用する。ランダム・イベント・シーケンス番号の発生プロセスは、ゲームがスタートする前に、すべてのゲーム参加者およびホスト・カジノに知らせて

あることに留意されたい。別々の協力ランダム・イベントの発生プロセスを使用して、各ランダム・イベントを発生することもできる。この方法は、ある種の形のカジノのゲーム参加者の共謀を防止することができるという利点がある。

4. ホスト・カジノは、ランダム・イベント・シーケンス番号を増大し、以降のランダム・ゲーム・イベントを生成するために使用するためにそれを記憶する（ステップ6へ行く）。

確定的ゲーム・イベント処理

5. ゲーム・イベントが、確定的ゲーム・イベントである場合には、ホスト・カジノは、確定的ゲーム・イベントを生成する。チェスの駒を移動することは、確定的ゲーム・イベントの一例である。ゲームの終了は、確定的ゲーム・イベントである（ステップ32へ行く）。

ゲーム・イベント処理

6. ホスト・カジノは、現在のゲーム状態を更新するために、ゲーム・イベントを使用する。

7. ホスト・カジノは、ゲーム参加者のパソコンに、現在のゲームの状況を知らせる。ある場合には、現在のゲームの状態の一部だけが、各ゲーム参加者のパソコンに送られ、その部分は異なる部分でもよいことに留意されたい。（みんながカードが配られたことを知っているが、一人のゲーム参加者だけが配られたカードの内容を知っていて、他のゲーム参加者は、あるイベントが発生したが、その内容を完全には知らないポーカーの場合のように）

8. 各ゲーム参加者のパソコンは、受信したゲーム・イベントまたはゲーム状態更新に基づいて、現在のゲーム状態のその知識を更新する。そうできる場合には、ゲーム参加者のパソコンは、また、それがゲームの規則と一致しているかどうかをチェックするために、ゲーム状態を再検討する。

ゲーム参加者の行動の選択

9. ゲーム参加者は、四つのタイプの行動の中の一つを選択することができる。補足協力ランダム・シード発生（ステップ10）、ゲーム参加者の決定（ステップ11-24）、秘密の公開（ステップ25-27）または秘密の確認（ステップ29-30）。補足協力ランダム・シード発生は、ポーカーまたはブラックジ

ヤックの際の、カードのデッキをもう一度切る行為を含む。

補足協力ランダム・シード発生

10. 補足協力ランダム・シード発生は、ゲーム参加者またはホスト・カジノによりスタートする。このプロセスは、ゲーム設定プロセス（ステップ20-36）のところで説明したプロセスと同じものであり、補足ゲーム・シードを生成するのに使用される。この活動は、カード・ゲームの際の「新しいデッキ」の要求、またはクラップスの際の「新しいダイス」の要求に似ている。このプロセスは、ゲーム参加者が目で見ることができる状態で、すなわち隠さないで行うことができる。（ゲーム参加者のパソコン上のアプリケーションは、プロセスのいかなるステップも表示しないで、すべてのステップを完了する。しかし、情報はゲーム参加者のゲーム・ログ内にログされる（ステップ32に行く）。

ゲーム参加者の決定

11. ゲーム参加者は、自分のパソコンにより提示された一組の可能な決定の中から、または現在のゲーム状態およびゲームの規則に基づいて、ホスト・カジノからある決定をする。ゲームの規則は、ゲーム参加者の入力および共通の規則に基づいて、ゲームの結果を得るために、予め定めた一連のプロセス・ステップである。例えば、ブラックジャックのゲームの規則は、各ゲーム参加者にカードを配り、ゲーム参加者に「カードをもう一枚配ること」または「パス」ができるようにし、そのカード全体の数が21を超えたゲーム参加者を「降ろし」、手の「分割」を許す等の一連のステップからなる。入手できるゲーム実行ソフトウェアの任意のバージョンをゲームの規則として使用できるようにすることができる。ゲーム参加者の決定は、（賭けること、ゲームの駒の移動、または競売または取引セッションの際の入札のような）確定的行動であってもよいし、またはホスト・カジノに対する、（ダイスを振る行為のような）ランダム・イベントを生成するようにとの要求であってもよい。すべてのランダム・イベントは、ホスト・カジノにおいて、実際に、実行されるので、ゲーム参加者は、ランダム・イベントを生成するように、カジノに要求する。クラップスの場合には、このことは、クルピエにダイスを振るように要求しているゲーム参加者と同じである。

12. ゲーム参加者が行なおうとしている決定が、合法的なものでない場合には

、ゲーム参加者のパソコンは、その決定を拒否する。

13. ゲーム参加者のパソコンは、合法的な決定属性を検索する。ゲーム参加者の決定は、いくつか属性を持つことができる（表3参照）。使用できる属性は、ゲームの規則および現在のゲーム状態によって決まる。決定は公開のものでも、秘密のものでもよい。決定は、「賭け」「カードの選択」、「カードを引くこと」、「ダイスを投げること」等のようなゲームの規則に基づく「決定タイプ」を持つ。決定タイプは、複数の数値を持つことができる。「カードを引く」という決定は、「3枚のカードを引きなさい」というように、ある特定の数のカードを引くことができるように、一つのパラメータを持つことができる。秘密の決定の場合には、追加の数値、すなわち、「プレイ活動の内容の非可逆的変形」が使用される。

14. ゲーム参加者は、決定タイプおよび決定数値を決定し、それを選択するか、自分のパソコンに入力する。

15. ゲーム参加者のパソコンは、決定タイプおよび決定数値をゲーム活動の内容に挿入する。

16. ゲーム参加者は、決定が秘密の決定であるのか、公開の決定であるのかを判断し、その情報をパソコンに入力する。秘密の決定は、ゲーム参加者および賭博場だけに知らされる。このことは、ゲームの規則に基づいて、ゲーム参加者のパソコンにより自動的に決定される。ゲーム参加者が秘密の決定をしたという情報は、ある種のゲームの場合には、他のゲーム参加者にとって役にたつ場合があるので、これは、ゲーム活動の内容に置かれる「NO DECISION」決定により保護することができる。秘密の決定は、秘密の移動または駒を置くことであってもよい。「バトルシップ」というゲームは、駒の置く場所を秘密にするゲームのおなじみの例である。

17. 決定が秘密である場合には、ゲーム参加者のパソコンは、ゲーム活動の内容の非可逆的変形を計算する。

18. ゲーム参加者のパソコンは、ゲーム活動の内容をホスト・カジノに知らせる。決定が秘密なものである場合には、ゲーム参加者のパソコンも、ホスト・カジノに、ゲーム活動の非可逆的変形を知らせる。ある種のゲームは、以降の「秘

密公開」中のゲーム内の後まで、またはゲーム確認プロセスまで、ホスト・カジノと共有していない秘密の決定をサポートすることができることに留意されたい。この特徴は、ホスト・コンピュータのないゲームの場合も真である。

19. ゲーム活動の内容が、非合法的な決定を示している場合には、ホスト・カジノは、その決定を拒絶し、カジノの正式な契約に従って、適当な行動をとる（ステップ33へ行く）。

20. ホスト・カジノは、賭博場ゲーム・ログ内にこの情報を記憶する。

21. 決定が公開のものである場合には、ホスト・カジノは、ゲームの規則に従って、他のゲーム参加者に、ゲーム活動の内容を通知する。この通知は、ゲーム活動の内容を転送することにより、またはゲーム・イベントまたは更新したゲーム状態を送ることにより行われる。可能な場合には、他のゲーム参加者は、転送した決定の合法性をリアルタイムで再検討する。決定が非合法的なものである場合には、ゲーム参加者は、ホスト・カジノに直ちに通知し、ゲーム参加者のゲーム・ログ、およびゲーム参加者例外ログ内にその情報を記憶する。行った他の行動は、カジノの正式な契約に従って行われる（ステップ24に行く）。

22. 決定が秘密なものである場合には、ホスト・カジノは、プレイ活動の内容が、プレイ活動の内容の容非可逆的変形を生成するために使用されたかどうかを確認する。確認できなかった場合には、ホスト・カジノは、決定を拒絶し、カジノの正式な契約およびゲームの規則に基づいて、適当なステップを行う。

23. ホスト・カジノは、ゲームの規則に従って、他のゲーム参加者に、ゲーム活動の内容の非可逆的変形を送る。

24. ホスト・カジノは、ゲームの規則に従って、ゲーム状態を更新するためにこの情報を使用し、ゲームを続行する（ステップ32へ行く）。

ゲーム参加者による秘密の公開

25. 規則またはゲーム参加者の判断で要求された場合には、秘密は公開される。ゲーム参加者は、また、ゲームの規則に従って、他のゲーム参加者に秘密を公開するように要求することができる。秘密は、秘密を生成したゲーム参加者および賭博場だけが知っている、ゲーム参加者の決定である（ステップ16-18参照）。「バトルシップ」の前の例を使用して、船が沈没した場合には、ゲーム参

加者は、一緒にボード上の船の位置を形成している、一組の位置を送ることによりその位置を明らかにする。

26. ゲーム参加者が、秘密を公開することを決めた場合には、ゲーム参加者は、秘密の決定の、ゲーム活動のシーケンス番号を最小として使用して、ホスト・カジノに特定の秘密を通知するために、自分のパソコンを使用する。ゲームの規則に従って、一人、数人、またはすべての他のゲーム参加者に、秘密を公開することができる。

27. 実際には、秘密は、ホスト・カジノにより公開される。ホスト・カジノは、ゲームの規則に従って、秘密を公開することができるかどうかを判断するためにゲーム活動のシーケンス番号をチェックする。その秘密が公開できないものである場合には、ホスト・カジノは、ゲームの規則およびカジノの正式な契約に基づいて適当な行動をとる（ステップ33に行く）。

28. ホスト・カジノは、適当なゲーム参加者のパソコンに、秘密の決定のゲーム活動の内容に対応する、ゲーム・プレイ・データを送る（ステップ32に行く）。

公開された秘密の確認

29. 他のゲーム参加者の秘密の決定に対する、ゲーム活動の内容を受信しているゲーム参加者のパソコンは、受信したゲーム活動の内容の非可逆的変形を計算し、それをゲーム参加者が、ゲーム中前に受信した、ゲーム活動の内容の非可逆的変形と比較する。

30. 確認できなかった場合には、ゲーム参加者は、ホスト・カジノに通知するために自分のパソコンを使用し、カジノの正式な契約および任意の規制オプションに基づいて、適当な行動をとる（ステップ33へ行く）。

31. 確認ができた場合には、ゲーム参加者は、ゲームを続行する。

ゲーム参加者の活動の処理

32. このシーケンスは、ゲームが終了し、ホスト・カジノが、すべてのゲーム参加者に、結果を通知するまで続行される（ステップ1に行く）。その後で、カジノおよびゲーム参加者は、ゲーム確認プロセスに移行する。

ゲーム・プレイの例外処理

33. ホスト・カジノまたはゲーム参加者のパソコンは、ゲーム中、他の参加者に、ゲーム・プレイ・プロセス中に起こるすべての障害を通知する。これらの障害は、適当なゲーム・ログおよび例外ログ内にログされる。障害が起こると、ゲーム・プレイ・プロセスを再スタートし、ゲーム・プレイ・プロセスをある既知の状態に戻すか、またはプロセスおよびゲーム・セッションを終了するために処理が行われる。この処理は、ゲーム参加者がホスト・カジノに登録した時、自分が同意したゲームの規則および正式な契約により決定される。

【0046】

2. 4 ゲームの確認

ゲームの確認とは、ゲームが終了した後で、すべてのゲームが正しく行われたことを確認することである。この確認は、ゲームから任意の秘密を公開するステップから始まり、ゲームの規則が破られなかったことを確認するステップで終わる一連のステップである（図14）。表4は、このプロセスのためのデータ・シーケンスを示す。

表4

ゲームの確認のデータグラムの内容

【表5】

フィールド名	説明	データ・タイプ
ヘッダ		
ギャンブル参加者ID	ギャンブル参加者の一意の識別子	整数
他のギャンブル参加者IDの組	そのギャンブルの、すべてのギャンブル参加者の、一意の識別子のリスト	整数の組
賭博場ID	賭博場の一意の識別子	整数
ギャンブル名	プレイ中のギャンブルのタイプの一意の識別子	賭博場が認識したプレイできるギャンブルの一覧表
ギャンブルID	プレイ中の特定のギャンブルの一意の識別子	整数
ギャンブル・プロトコル確認ペイロード		
ギャンブル・プロトコル確認の内容	ギャンブルIDにより指定されたギャンブルを再構成するために必要な情報。この情報は、確認プロセスのために、ギャンブル参加者と賭博場との間で通信された情報を必要とする、各イベントに対する一連のデータ構造体である。	ギャンブル・シーケンス番号、確認活動のタイプ、および活動情報の内容を含む、各素子を持つ一組のデータ構造体
ギャンブル活動シーケンス番号	特定のギャンブル内のイベントまたは決定に対する一意の番号。賭博場だけが設定。ギャンブルのプレイ部分から、古いイベントを再度呼び出すために、この確認プロトコル内で使用。	整数
確認活動のタイプ	これがギャンブル・シードの確認か、または秘密の確認かを識別する数値（決定またはイベント）	（ギャンブル・シードの確認または秘密の確認の）一覧表
ギャンブル・プロトコル確認の例外情報	すべてのギャンブル参加者および賭博場への、ギャンブル・プロトコルの正しい実行へのすべての例外の通知	データ構造 ⁽¹⁾

(1) すべてのサポート・パラメータを含むための、ゲーム参加者の決定に対して一意のデータ構造

表4（続き）

ゲームの確認のデータグラムの内容

下記の追加情報は、協力シード活動の確認のために使用される。

【表6】

フィールド名	説明	データ・タイプ
ギャンブル参加者のランダム・シード	協力ランダム発生の際に使用するための、ギャンブル参加者により供給される乱数。この乱数は、ギャンブル参加者が発生したとき記憶されたもので、シード確認プロセス中、ギャンブルの再構成が行われる際に使用される。	賭博場とのギャンブル参加者の通信のためだけに指定される2進シーケンス
ギャンブル参加者のランダム・シードの組	協力ランダム発生の際に使用するための、ギャンブル参加者IDを持つ、一組のギャンブル参加者が供給する乱数を識別する一組のペアの形をしているデータ（ギャンブル参加者ID、ランダム・シード）。このデータは、ギャンブル・シードを再構成するために、確認段階中に使用される。	整数および2進シーケンスの一組の順番に並べたペア
賭博場のランダム・シード	協力ランダム発生の際に使用するための、ホスト・カジノが発生した乱数。ギャンブル・シードの再構成の確認段階まで、ギャンブル参加者に供給されない。	2進シーケンス
賭博場のランダム・シードの非可逆的変形	協力ランダム発生のために、賭博場が使用するランダム・シードの非可逆的変形。ギャンブル参加者は、シード生成以来、賭博場のランダム・シードが正しく、また変化していないことを確認するために、確認段階中にこれを使用する。	2進シーケンス

下記の情報は、他の秘密の活動を再構成するために必要なものである。

【表7】

フィールド名	説明	データ・タイプ
プレイ活動の内容	イベント、決定または公開活動の内容	データ構造
プレイ活動の内容の非可逆的変形	イベント、決定、公開、または賭博活動の内容の非可逆的変形	データ構造

【0047】

ゲーム設定に関する節、およびゲーム・プレイに関する節全体にわたって説明したように、データは、確認をサポートするために、ログ内に記憶済みである。賭博場イベントおよびゲーム参加者の決定に関するデータは、適当なゲーム・ログから検索され、一緒にゲームを構成するイベント、および決定の全シーケンスを再構成するために使用される。この情報の中のあるものは、（特定のゲームおよびゲームの規則に従って）、確認段階中にだけ公開することができる。この情報は、ゲームの各ステップを再構成し、ゲームの設定およびプレイ・プロセスおよびゲームの規則と照合して確認できるように、ゲーム中に、ゲーム・ログ内に蓄積された情報と結合される。ゲームの確認プロセスの詳細の全体は、ゲーム参

加者に表示されない。しかし、上記情報は、各ゲーム参加者のパソコン上に確かに記憶される。確認ソフトウェアは信頼できるものでなければならないので、このソフトウェアは、独立エンティティまたは規制団体が供給するものか、上記機関により証明されたものでなければならない。

【0048】

ゲームの確認の開始

1. ゲームが終了すると、ホスト・カジノは、各ゲーム参加者に、「ゲーム終了」というゲーム・イベントを送る。ホスト・カジノは、ゲーム確認プロセスを始動する。

2. 各ゲーム参加者のパソコンは、ゲーム・イベントを処理し、そのゲーム参加者に通知し、ゲーム確認プロセスを始動する。

ゲーム・シードの確認

3. ホスト・カジノは、賭博場ゲーム・ログから、賭博場ゲーム・シードを検索する。

4. ホスト・カジノは、各ゲーム参加者に、賭博場ゲーム・シードを送る。ホスト・カジノは、そうしたい場合には、賭博場ゲーム・ログから、ゲーム参加者のゲーム・シードを検索し、そのゲーム・シードを各ゲーム参加者のパソコンに送る。（これらシードは、ゲーム設定プロセス中に送られたものである。）

5. ホスト・カジノは、賭博場ゲーム・ログから、ゲーム・シードを検索する。

6. ホスト・カジノは、各ゲーム参加者のパソコンに、ゲーム・シードを送る。ゲーム中に、複数のゲーム・シード、および賭博場のランダム・シードが使用された場合には、上記シードはすべて検索され、この時点で送られる。

7. 各ゲーム参加者のパソコンは、新しく受信した賭博場ランダム・シードの非可逆的変形を計算し、それを、自分のゲーム参加者のゲーム・ログから検索した、賭博場のランダム・シードの非可逆的変形と比較する。（これは、ゲーム設定プロセス中に供給される。）

8. 比較ができなかった場合には、ゲーム参加者は、その事実をホスト・カジノに通知し、ゲーム参加者とカジノとの間の正式な契約に従って、（規制団体へのコンタクトを含む）適当な行動をとる。ゲーム参加者のパソコンおよびホスト・

カジノは、また、適当な例外ログ内にこの情報をファイルする。

9. 比較できた場合には、ゲーム参加者のパソコンは、ゲーム・シードを構成するために、協力ゲーム・シード発生プロセス、新しく受信した賭博場のランダム・シード、および（各ゲーム参加者のゲーム・ログから今受信したか、検索した）すべてのゲーム参加者のゲーム参加者のランダム・シードを使用する。このプロセスは、ゲーム中に使用した各ゲーム・シードに対して反復して行われる。ゲームがスタートする前に、すべてのゲーム参加者およびホスト・カジノは、協力ゲーム／シード発生プロセスを知っていることに留意されたい。ゲーム・シードを再構成するということは、ゲームが終了してから、カードのデッキを切ることができること、またはダイスの回転のシーケンスをもう一度やり直すことができるのと同じことであり、ブラックジャックまたはポーカーのゲームからの、すべての活動を再構成することができることと同じことである。

10. 各ゲーム参加者のパソコンは、新しく構成したゲーム・シードを、ホスト・カジノから受信したゲーム・シードと比較する。ゲーム参加者のパソコンは、また、ゲーム・シードの非可逆的変形を、ゲーム参加者の、ゲーム参加者ゲーム・ログから検索した、ゲーム・シードの非可逆的変形と比較する。ゲーム・シードは、シード再構成プロセスにより確認されるので、ゲーム・シードの非可逆的変形を供給する必要は全然ないことに留意されたい。このことは、性能上の理由だけで行われる。

11. どちらの比較もできなかった場合には、ゲーム参加者は、その事実をホスト・カジノに通知し、ゲーム参加者とカジノとの間の正式な契約に従って、（規制団体へのコンタクトを含む）適当な行動をとる。ゲーム参加者のパソコンおよびホスト・カジノは、また、適当な例外ログ内にこの情報をファイルする。

12. 任意のゲーム参加者により保持されている、公開されていない秘密決定がある場合には、各ゲーム参加者のパソコンは、自分の各ゲーム参加者のゲーム・ログからこれら決定を検索し、それをホスト・カジノに通知する。このことは、プレイ活動の内容およびゲーム活動のシーケンス番号の両方を含む。ゲーム、「バトルシップ」中、ゲーム参加者は、すべての船の位置を他のゲーム参加者に供給する。（しかし、本当に供給する必要があるのは、「まだ沈んでいない」船の

ものだけである。)

13. ホスト・カジノは、賭博場ゲーム・ログから、すべての残りのまだ公開されていない秘密の決定を検索する。この検索は、プレイ活動の内容およびゲーム活動のシーケンス番号の両方を含む。

14. ホスト・カジノは、新しく受信した秘密の決定に対するゲーム活動の内容の非可逆的変形を計算し、それを、ホスト・カジノが賭博場ゲーム・ログから検索した、対応するゲーム活動の内容非可逆的変形と比較する。ホスト・カジノは、また、賭博場ゲーム・ログ内に新しく受信したゲーム活動の内容を記憶する。

15. 比較できなかった場合には、ホスト・カジノは、ゲーム参加者に通知し、カジノとゲーム参加者との間の、正式な同意に基づいて適当な行動をとる。この行動は、すべての賭金の没収、罰金、ゲーム参加者のカジノへの出入りの禁止等を含むことができる。ホスト・カジノは、また、すべての他のゲーム参加者に通知し、カジノとゲーム参加者との間の、正式な同意に基づいて適当な行動をとる。この行動は、違反したゲーム参加者が支払った金またはペナルティの返却を含むことができる。

16. 比較できた場合には、ホスト・カジノは、ゲームのその時点で、ゲームの規則およびゲーム状態に従って、その決定が合法的なものであったことを確認する。決定が非合法的なものであった場合には、ホスト・カジノは、ゲーム参加者に通知し、カジノとゲーム参加者との間の、正式な同意に基づいて適当な行動をとる。ホスト・カジノは、また、すべての他のゲーム参加者に通知して、カジノとゲーム参加者との間の、正式な同意に基づいて適当な行動をとる。

17. ホスト・カジノは、すべての残りのまだ公開されていない秘密の決定をすべてのゲーム参加者に通知する。ホスト・カジノは、また、すべての新しく受信した秘密の決定をすべてのゲーム参加者に転送する。

18. 各ゲーム参加者のパソコンは、新しく受信した秘密の決定に対する、ゲーム活動の内容の非可逆的変形を計算し、それを、ホスト・ゲーム参加者が、その各ゲーム参加者ゲーム・ログから検索する、対応するゲーム活動の内容非可逆的変形と比較する。

19. 比較できなかった場合には、ゲーム参加者は、その事実をホスト・カジノ

に通知し、ゲーム参加者とカジノとの間の、正式な契約に従って、（規制団体へのコンタクトを含む）適当な行動をとる。ゲーム参加者のパソコンおよびホスト・カジノは、また、その各例外ログ内にこの情報をファイルする。

20. 比較できた場合には、各ゲーム参加者は、自分の各ゲーム参加者のゲーム・ログ内に受信したゲーム参加者の決定を記憶する。この時点で、各ゲーム参加者は、ゲームからのすべてのゲーム参加者の決定を持っていることに留意されたい。

ランダム・イベントの再構成

21. 各ゲーム参加者は、すべてのランダム・ゲーム・イベントを再構成するために、自分の各ゲーム参加者ゲーム・ログおよびゲーム・シード（複数ある場合には、複数のゲーム・シード）を使用する。このゲーム・シードにより、カードを切る行為またはダイスの投擲をもう一度行うことができる。確定的ランダム発生プロセス、または協力ランダム発生プロセスは、実際に、特定のランダム・イベント（カードを切る行為またはダイスの投擲）シーケンスを再構成する。

22. ゲーム参加者は、すべてのランダム・ゲーム・イベントを計算するために、ゲーム・シードを使用し、それを、ゲーム参加者のパソコンが、自分のゲーム参加者のゲーム・ログ内に記憶したランダム・ゲーム・イベントと比較する。各ゲーム参加者のパソコンは、自分の各ゲーム参加者ゲーム・ログ内に新しく計算したランダム・ゲーム・イベントを記憶する。ゲームを行う前に、ホスト・カジノおよびすべてのゲーム参加者は、使用した確定的ランダム・プロセスを知る。

23. 比較できなかった場合には、ゲーム参加者は、その事実をホスト・カジノに通知し、ゲーム参加者とカジノとの間の正式な契約に従って、（規制団体へのコンタクトを含む）適当な行動をとる。ゲーム参加者のパソコンおよびホスト・カジノは、また、その各例外ログ内にこの情報をファイルする。この時点で、各ゲーム参加者は、ゲームからのすべてのゲーム・イベント（ランダム・イベント、および確定的イベントの両方）を持っていることに留意されたい。

規則の確認

24. 各ゲーム参加者のパソコンは、各ゲーム参加者のゲーム・ログから、初期ゲーム状態を検索し、各ゲーム参加者の決定および各ゲーム・イベントが、ゲー

ムの規則に適合していることを確認するために、すべてのゲーム参加者の決定、および自分のコンピュータ上に現在存在している、ゲーム・イベントとの組合せを使用する。この確認は、ゲーム参加者が知らない活動、すなわち、秘密の移動または駒の設置、および（ポーカーの場合のように）カードの引き抜きに対して、この時点でだけ行うことができる。

25. 規則の確認ができなかった場合には、ゲーム参加者は、その事実をホスト・カジノに通知し、ゲーム参加者とカジノとの間の正式な契約に従って、（規制団体へのコンタクトを含む）適当な行動をとる。ゲーム参加者のパソコンおよびホスト・カジノは、また、その各例外ログ内にこの情報をファイルする。

26. 規則の確認ができた場合には、ゲーム確認プロセスは成功したのであり、各ゲーム参加者は、その事実をホスト・カジノに通知する。ホスト・カジノは、賭博場のゲーム・ログ内にその情報を記憶する。ホスト・カジノは、また、その事実を他の各ゲーム参加者に通知する。各ゲーム参加者は、他のゲーム参加者が確認した確認を自分の各ゲーム参加者のゲーム・ログ内にログする。その後で、各ゲーム参加者は、他のゲームをスタートすることができる。

ゲームの確認の例外処理

27. ホスト・カジノまたはゲーム参加者のパソコンは、ゲーム中、他のゲーム参加者に、ゲーム確認プロセス中に起こるすべての障害を通知する。これらの障害は、適当なゲーム・ログおよび例外ログ内にログされる。障害が起こると、ゲーム確認プロセスを再スタートさせ、またはある既知の状態にゲーム確認プロセスを回復させるために、処理が行われる。ゲーム参加者は、そうしたい場合には、何時でも、規制要件およびゲーム参加者とカジノとの間の正式な契約にに基づいて、ゲーム・ログを記憶するように、カジノの要求されている限りは、ゲームを確認することができる。この処理は、ゲーム参加者がホスト・カジノに登録した時に、自分が同意したゲームの規則および正式契約により決まる。

ゲーム参加者の不公正な行為に対処するために、賭博場が、ゲーム確認プロセスとは別のなんらかの行動をとる可能性がある。同様に、ゲーム参加者が、賭博場または他のゲーム参加者による不公正な行為を検出した場合には、規制団体または法施行団体になんらかの行動をとる可能性がある。

【0049】

2. 5 ホストーゲーム参加者間の取引

ホストーゲーム参加者間の取引は、個々のゲーム・プロセス・ステップを信頼性の高い方法で処理する手段、およびゲーム参加者およびカジノが、ゲームの状態について同じ情報を必ず持つようにする手段を供給する（図15）。ホストーゲーム参加者間の取引のプロセスは、ゲーム参加者とホスト・カジノとの間で情報の交換が行われるプロセス内の大部分のステップのために使用される（図10参照）。これらのステップは、2. 1－2. 4節およびこれら節に対応する図面内に明示してある。表5は、このプロセスに対するデータ要件を示す。

表5

ホストーゲーム参加者間の取引データグラムの内容

【表8】

フィールド名	説明	データ・タイプ
ヘッダ		
ギャンブル参加者ID	ギャンブル参加者の一意の識別子	整数
賭博場ID	賭博場の一意の識別子	整数
取引きのタイプ	ギャンブル参加者かまたは賭博場である受信人のID	整数
取引きのデータ	これが承認されたギャンブル情報の通信、承認または確認であるかどうかについての識別。これらのタイプは、取引きの三つのステップからなるハンドシェイクの一部として、この順序で実行される。	一覧表（通信、通知、確認）の中の一つ
取引きデータ		
データ/時間	行われているギャンブルのデータと時間の指定。このデータ/時間は、取引きステップの時間に関連する。	データ構造
取引きのシーケンス番号	特定の取引き内のイベントまたは決定の一意の番号。賭博場だけが設定。取引きが承認されるまで指定されない。	整数
取引きのペイロード		
埋設プロセス・データグラム	カプセル収容ギャンブル・プロトコルを含む、取引きペイロード（2. 1-2. 4節）	データ構造（2. 1-2. 4節参照）
取引き応答情報	受信人に、プロトコルの正しい実行中の、現在行われている取引きステップを通知するために使用するコード。この情報は、通知情報であっても、例外情報であってもよい。	データ構造
身元確認データ		
署名および信頼性のデータ	公開キー署名および他の信頼性情報	2進シーケンス ⁽²⁾

(1) 身元確認または拒絶不能に対する実行の際にサポートされる、取引きプロトコルおよび任意の他の規格または市販の技術に対する一意のデータ構造。

(2) 特注フォーマットであるか、インターネット・タスク・フォース（IETF）X. 509 デジタル署名規格の規定に従って実行される。

【0050】

このプロセスは、ゲーム参加者とホストとの間で、データが必ず正しく移送されるようにするための三つのステップからなるハンドシェイク・プロトコルを使用する。上記プロセスは、また、非常に強力なデータ信頼性および拒否不能を供給するために、デジタル署名（3. 4. 3節）による身元確認を使用する。この特性は、サイン入りのメッセージの受信側が、そのメッセージを誰が送ったのかが分かることを意味する。受信側は、また、受信したメッセージが、送信側が送

ったものであることも分かる。署名は送信側が後で、自分がメッセージを送信したことを否定できないという別の特性も持つ。ホスト・カジノまたはゲーム参加者は、ホストーゲーム参加者間の取引きをスタートすることができるので、この説明では、取引きを開始し、データを供給している側に対して「送信側」という用語を使用し、上記データを受信している側に対して「受信側」という用語を使用する。ホストーゲーム参加者間の取引きプロセスは、一意の分散型 ゲーム実行要件に適合するように調整されている。このプロセスは、プロセス中の前のステップが失敗した場合に、データの再送信をサポートする。そうである場合には、取引きは、取引き中に、スタート地点または前のステップに戻るることができる。取引きは、そうしたい場合には、その各取引き活動ログ内に、ゲーム参加者またはホスト・カジノにより、そのプロセスの適当なステップ内にログし、記録することができる。このログは、ゲームの確認または法的／規制上の要件に適合するように、期間を延長して保管することもできるし、ゲームが行われている時間中だけ、または特定の取引きの間だけ保管することができる。各取引きは、ホスト・カジノが指定するシーケンス番号を含み、各ゲーム活動によりこの数字は増大する。日付けおよび時刻は、シーケンス番号が再使用されないように、十分に正確なものでなければならない。

カジノのセッションのスタート時において、ホスト・カジノは、任意のゲーム設定またはゲーム参加者の登録活動の前で、一人のゲーム参加者によるセッションのスタート時に、取引きシーケンス番号を指定する。

取引きの生成

【0051】

1. 送信側のコンピュータは、プロセス・ステップ・データグラムを検索する。
2. 送信側のコンピュータは、取引きヘッダを含む取引きデータグラムをフォーマットし、プロセス・ステップ情報を取引きペイロード内に挿入する。その後で、送信側は署名を計算し、取引き身元確認データ用の他の信頼性データをフォーマットする。送信側は、取引き活動ログ内に取引きデータグラムを記憶する。送信側は、必ずしも実際のデータグラムを記憶する必要はなく、なんらかの理由で取引きが失敗した場合は、データグラムを再構成するために、十分な情報を記憶

することができる。

3. 送信側は、取引きデータグラムを受信側に知らせる。

取引きの確認および承認

4. 受信側は、受信した取引きヘッダおよびペイロードにより、署名および他の身元確認情報を確認する。

5. 確認できなかった場合には、受信側は、取引きペイロード内に失敗したことを示す取引き応答情報データグラムをフォーマットする。

6. 確認できた場合には、受信側は、取引き応答情報データグラムをフォーマットする。このフォーマットは、フラグまたは受信側が受信した全取引きペイロードと同じように簡単に行うことができる。

7. 受信側は、その取引き活動ログ内に取引き応答情報データグラムを記憶する。

8. 受信側は、送信側に、取引き応答情報を含む取引きデータグラムを送る。

取引きの承認の確認

9. 送信側は、受信した取引きデータグラムを確認する。この確認は、使用する取引き応答情報のタイプにより異なる。

10. 送信側で確認出できなかった場合には、送信側は、受信側に受信側の応答を再度送信してくれるようにプロンプトしている、取引き応答情報データグラムをフラグする。このフォーマットは、送信側が、ある時間内に応答を受信しなかった場合にも行われる。

11. 送信側で確認できたが、受信側の初期確認ができなかった場合には、送信側は、元の取引きデータグラムを再度フォーマットする。日付け／時刻情報は変更することができるが、取引きシーケンス番号を変更する必要はない。

12. 送信側で確認することができ、受信側でも確認することができた場合には、送信側は、自分が受信側の初期応答を受信したという応答をフォーマットする。送信側は、取引きが成功したという事実を取引き活動ログ内に記憶する。

13. 送信側は、取引き応答情報データグラム情報を取引き活動ログ内に記憶する。

14. 送信側は、受信側に、取引き応答情報を含む取引きデータグラムを送る。

取引きの確認および終了

15. 受信側は、受信した取引きデータグラムを確認する。この確認は、使用する取引き応答情報のタイプにより異なる。

16. 受信側で第二の確認ができなかった場合には、受信側は、送信側に取引きデータグラムを再送信してくれるようにという要求を送る。受信側がある時間内に応答を受信しなかった場合にも、上記要求の送信が行われる。

17. 受信側で第二の確認を行うことができたが、送信側で確認できなかった場合には、受信側は、元の取引きデータグラムを再度フォーマットし、それを送信側に再送信する。日付け/時刻情報は変更することができるが、取引きシーケンス番号を変更する必要はない。

18. 受信側で第二の確認をすることができ、送信側でも確認することができた場合には、取引きは成功し、この事実が、取引き活動ログ内に記憶される。

取引きシーケンス番号の配布

19. ホスト・カジノが参加する第一の取引きステップ中に、それは、ゲーム参加者に対する次の取引きシーケンス番号を含む。

【0052】

2. 6 機密保護ホスト-ゲーム参加者間の通信

機密保護ホスト-ゲーム参加者間の通信の目的は、各ゲーム参加者と賭博場との間に、機密保護チャンネルを設定することである（図16）。表6は、このプロセスに対するデータ要件を示す。

表6

機密保護ホスト-ゲーム参加者間の取引きデータグラムの内容

【表9】

フィールド名	説明	データ・タイプ
ヘッダ・データ		
ギャンブル参加者ID	ギャンブル参加者に対する一意の識別子	整数
賭博場ID	賭博場に対する一意の識別子	整数
通信のタイプ	これがギャンブル取引なのか、または他の通信なのかの識別	一覧表
宛先ID	情報に対する他の宛先の一意の識別子	整数の組
通信ペイロード		
メッセージ内容	カプセル収容取引プロトコルを含む、選択した通信プロトコルに関連する通信データグラム（2. 5 節）	データ構造
通信の例外情報	他の当事者に、プロトコルの正しい実行に対する、すべての例外を知らせるために使用されるエラー・コード。宛先IDは、受信側アドレスとして使用される。	データ構造

【0053】

このプロセスは、（TCP/IPのような）普通のネットワーク通信プロトコルの一番上に位置し、ホストーゲーム参加者間の通信、および他のメッセージ通信の両方を送信するのに使用することができる（図17）。機密保護ホストーゲーム参加者間の取引プロセスは、ゲーム参加者とホスト・カジノとの間で情報の交換が行われる、大部分のプロセス・ステップのために使用される（図10参照）。これらステップは、2. 1-2. 5 節およびこれら節に対応する図面に明示してある。異なるゲーム参加者の間のすべての通信は、ホスト・カジノを通して転送される。ホスト・カジノは、ゲームの規則および正式な契約に基づいて、その通信の転送が、合法的なものであるかどうかを判断し、必要な場合には、ゲームの確認の際に使用するためにその通信をログする。

カジノのセッションのスタートのところで、

【0054】

1. ゲーム参加者のパソコンおよびホスト・カジノは、その通信の機密保護を行う目的で、一意のキーを生成するために、ある種の機構を使用する。
2. ゲーム参加者のパソコンおよびホスト・カジノは、両方の間のリンクを暗号化するために、上記の一意のキーを使用する。
3. ゲーム参加者は、機密保護通信リンク内で、ゲーム参加者登録プロセス中に開発した識別情報をホスト・カジノに送る。
4. ゲーム参加者識別情報が無効である場合には、ホスト・カジノは、セッション

ンを終了し、例外ログ内にその情報をログする。

5. ホスト・カジノは、ゲーム参加者に、対応する識別情報を供給する。この情報は、またゲーム参加者登録プロセス中に供給されたものである。

6. ホスト・カジノセッション識別情報が無効である場合には、ゲーム参加者はセッションを終了し、上記情報を例外ログ内にログする。

7. 上記識別情報が有効である場合には、機密保護ホストーゲーム参加者間の通信リンクが確立され、セッション中の以降のすべての通信に対して使用される。ゲーム参加者とホスト・カジノ間の各通信ステップの場合、

【0055】

1. 各メッセージ・タイプに対して、送信側は、メッセージ内容およびメッセージ・ヘッダを通信データグラムにフォーマットする。メッセージ・タイプは、取引データグラム、ゲーム参加者／賭博場間の通信、および他のゲーム参加者に転送されるメッセージを含むことができる。プロトコルは、日付／時刻情報をサポートしないことに留意されたい。賭博場は、クロックに対してマスタとしての働きをし、この情報を他のプロトコル情報と一緒に、ゲーム参加者に供給する。

2. 送信側は、マスタを暗号化する。

3. 送信側は、受信側にメッセージを送る。

4. 受信側は、メッセージを受信する。

5. 受信側は、メッセージ解読する。

6. 受信側は、メッセージを処理する。

7. ホスト・カジノのパソコン、またはゲーム参加者のパソコンは、セッション中の他のゲーム参加者に、機密保護ホストーゲーム参加者間の通信プロセス中に起こるすべての障害を知らせる。これら障害は例外ログ内にログされる。

【0056】

3. 動作理論

不公正な行為のないことを立証できる分散型ゲーム実行取引処理システムの四つの技術的設計の特徴は、公正なゲーム進行手続処理システムをサポートする。

1. ゲーム取引処理システムのアーキテクチャは、その内部で広い範囲のゲー

ム取引システムを記載することができる構造体を供給する。

2. 信頼レフリー・モデルは、ゲーム取引プロセスを確実に不公正な行為サマののないものにする方法を供給する。

3. 不公正な行為のないモデルは、詐欺を防止するためのシステムの能力および限界を示す。

4. 数学的技術的素子は、プロトコルの実行の際に使用され、周知の数学的および暗号化技術に基づいて構成される。

3. 1 ゲーム取引処理システムのアーキテクチャ

不公正な行為が行われなかったことを実証することができる、分散型ゲーム取引処理システムが動作するのは、ゲーム取引処理システムが、一組の規則により制御される相互作用の構造化シーケンスである。一般的な取引処理システムは、複数のゲームとみなすことができる。上記システムは、(勝者の決定のような)ある結論に到達するために、構造化された方法(規則)により相互に作用する、一つまたはそれ以上の当事者(ゲーム参加者)を含む。以下に、ゲームという観点から取引処理システムを説明する。ゲームには五つの主要な素子がある。これら素子について以下に説明し、図18に示す。

【0057】

1. イベント — ゲームの結果に影響を与えるゲーム中に発生する活動。イベントは、ゲーム参加者の決定に対抗するものとして、ゲームの規則により決定される。

2. 決定 — ゲームの結果に影響を与える、ゲーム中のゲーム参加者による選択。

3. 規則 — 合法的な相互作用、およびゲーム・イベントと、ゲームを、ある状態から以降の状態へと進行させることができるゲーム参加者の決定との組合せ。規則は、ゲームの開始と終了とを指定するために使用される。規則は、ゲームの勝者を指定するために使用される。(例えば、マスク出版の「デラックス・カジノ・パク16」のような)任意の入手できるソフトウェアを規則として使用できるように改造することができる。

4. 環境 — 競技者にとってゲームを魅力的にし、また(モノポリのゲーム内

のボードを見て) ゲームの規則および現在の状態を容易に理解できるようにするための、視覚的属性、聴覚的属性およびその他の属性。ゲーム環境は、異なる個々のゲーム参加者にとって異なる場合がある。何故なら、ゲーム参加者は、完全なゲーム状態に、アクセスすることができないからである。

5. 状態 — ゲーム状態は、状態情報、現在の可能なゲーム・イベント、およびゲーム参加者の決定からなる。状態は、過去のすべてのイベント、および既知の出発点から、ゲーム中に行われた決定の蓄積された結果である。各イベントまたは決定により、ゲーム状態が変化する。個々のゲーム参加者は、必ずしもゲーム状態を完全に知っているわけではない。

この枠組みにより、大部分のゲーム取引プロセスを、規則の施行を自動化することができ、分散型環境またはネットワーク環境で、ゲーム取引システムの処理を行うことができるようにする、ネットワークゲーム実行取引処理プロトコルを使用することができる、組織的フォーマットで記述することができる。

【0058】

3. 2 信託レフリー・モデル

信託できるゲーム取引処理システムは、ゲーム参加者が、規則が既知のものであり、施行されていると信託することができるシステムである。この信託には二つの面がある。他のゲーム参加者の信託およびレフリー自身の信託である。

【0059】

レフリーは、ゲーム参加者のすべての活動(決定およびゲーム参加者間の通信)をモニタし、ゲーム取引処理システムの規則、および現在の取引処理システムの状態を完全に理解することにより、確実に、すべての行動をゲーム取引処理システムの規則に適合させる。それ故、レフリーは、取引処理システムの任意の所与の時点で、どんなゲーム参加者の決定、およびどんな取引処理システム・イベントが、可能であるのかを知ることができる。レフリーは、いかなる非合法的な行動も起きさせない。規則違反が行われようとしている場合には、レフリーは、直ちに介入して、(同様に、規則により定められた)適当な行動をとる。これら行動は、ゲーム参加者に他の選択を行うようにうながすことから、取引プロセス・ゲームを終了させ、ゲーム参加者に対してなんらかのペナル

ティを課することまで、広い範囲にわたることができる。

【0060】

「レフリーの信託」は、ネットワークゲーム取引処理プロトコルの確認部分により解決される実行チャレンジである。ゲーム参加者は、レフリーの個々のコピーを持つ。レフリーというのは、ゲーム取引処理システムの規則を完全に理解していて、遑って（または、場合によっては、直ちに）ホストにより制御されている取引処理システム・レフリーが正しく動作していること、ゲーム自身のバランスがよくとれていることを確認することができるアプリケーションである。このアプリケーションは、個々の規制団体により供給することができるし、上記団体により認定することができる。それ故、このゲーム参加者が制御するレフリー・アプリケーションは、ゲーム参加者が、取引処理システムを確認するのに使用する、ゲーム参加者取引処理システム・ログと一緒に、ホストまたは他のゲーム参加者に対する、規則違反のすべての申し立てをサポートするために使用することができる。

【0061】

ホストのいない取引処理システムにおいては、二人またはそれ以上のゲーム参加者は、それぞれ、他のゲーム参加者がイカサマをしないことを確認するために、自分のレフリー・アプリケーションを使用することができる。

【0062】

3. 3 不公正な行為のないモデル

取引システムでは、二つのタイプの不公正な行為防止が行われている。取引に関する不公正な行為防止と、人間に関する不公正な行為防止である。取引に関する不公正な行為防止は、取引および取引処理規則のステップ、すなわち、システムのすべてのものに関する不公正な行為防止である。本明細書においては、取引のステップの保護について詳細に説明する。取引処理規則は、取引に関する当事者間の共通の同意である。分散型システムにおいては、当事者が、同じ規則を使用していることを知るのは特に難しい。規則セット登録のある種の手段が必要であり、そのため、規則のいくつかの組にラベルを貼る共通な方法がある。（ブラックジャック — 100回から300回使用したら、カード入

れを焼却する8のデッキ・カード入れを使用するラスベガス・スタイル」) これらの規則の組のラベルを知らせ、身元を確認するための手段が必要になる。

【0063】

人間に関する不公正な行為防止は、処理システム自体の外側での取引に含まれる個人の行動である。都合の悪いことに、取引システムの外部での個人による公正な行為の行動を自動化し、身元を確認し、または他の方法で強制的に行わせる方法はない。個人は、共謀したり、所与の取引に対して許可されていない他の活動を行うことができる。取引システム、特に、分散型システムで、個人が適当な行動を取るようにしむける主な手段は、契約と監視である。契約は、取引システムの規則の違反に対する制裁を明記しなければならない。監視とは、異常な行動をしないように個人の行動を観察することである。さらに、分散型システムの場合には、停電、接続の切断、およびその他の問題も解決しなければならない。解決しなければならない特定の問題は、(ゲームに負けそうなゲーム参加者のような 不利な結果を避けるために、取引を中断しようとしている、取引を行っている当事者である。

【0064】

3. 4 技術的素子

ネットワーク・ゲーム実行取引処理プロトコルのために使用される、四つの主要な技術的素子がある。ランダム化装置、非可逆的変形、署名およびハッシュ機能は、周知の数学的技術である。協力シード発生は、乱数を協力して発生させるための、ランダム化装置と非可逆的変形との新しい組合せである。

【0065】

3. 4. 1 ランダム化装置

本発明は、二つの目的のためにランダム化装置を使用する。第一は、ランダム化装置は、賭博場およびゲーム参加者が使用するシードを発生するために使用される(2. 2-2. 3節)。これらのランダム化装置は、確定的乱数であってもよいし、真の乱数であってもよい。第二に、確定的ランダム化装置は、ゲーム中に、ランダム・イベントをシーケンシャルに発生するために使用される。確定的ランダム化装置は、ゲーム終了後、上記シーケンスを再構成することができる

ように、ランダム・イベントを発生するために使用される。

【0066】

ランダム化装置は、予測できない情報を発生する。コンピュータをベースとするランダム化装置の場合には、このことは、通常、発生したシーケンスを知っていても、次になにが発生するかを予測することができないような方法で、複数の0および複数の1が発生することを意味する。ランダム化装置には二つのタイプがある。すなわち、真のランダム化装置と確定的ランダム化装置（または、疑似ランダム化装置）である。真のランダム化装置は、そのランダム・データを発生するために、ある種のノイズ源を使用している。確定的ランダム化装置は、疑似ランダム・データを発生するために、数学的機能とシードを使用する。シード上の数学的機能の出力は、疑似ランダム・データ（一連の0と1）である。その後で、シードは、通常、ランダム・データを引続き発生するために、ある種の方法で更新される。優れた確定的ランダム化装置は、ランダム化装置機能の所与の知識および発生したシーケンスであるが、シードでないものである。計算により、次に発生する疑似ランダム・データを推測することはできない。そのため、ゲーム・シードは、ゲームが終了するまで、明らかにされない。

【0067】

2進ランダム・ストリームは、任意の必要な分布を発生するために、使用することができる。0から $N-1$ までの数値の均一な分布は、ランダム・ストリームからの $\log_2 N$ ビット・シーケンスから発生することができ、結果が（ N より大きいか、または等しい）領域の外にある場合には、新しい数値を発生する。例えば、52枚の組のカードからの数値は、乱数ゼネレータからの、6ビットのシーケンスを使用して、発見することができる。この6ビットの数字は、0から63までのある数字である。発生した数値が、1から52までの範囲内に含まれていない場合には、1から52までの範囲内の数値が発生するまで、新しい6ビットのシーケンスが選択される。複数のカードを配らなければならない場合には、次の数字は、1から51までの範囲から選択され、次に、1から50までの範囲から選択される。以下同様である。均一な分布を組み合わせることにより、均一でない分布を形成することができる。

【0068】

3. 4. 2 非可逆的変形

非可逆的変形は、その関数の出力がある場合には、入力を計算により再構成することができる属性を持つ数学的関数である。（簡単な例としては、通常の紙の電話帳がある。所与の名前の電話番号を発見するのは簡単だが、掲載されているすべてのものが電話番号であり、電話帳のコピーである場合には、その名前を発見するのは非常に難しい。）すべての非可逆的変形は、入力データを「合体」する。すなわち、可能な出力の数は、可能な入力の数より少ない。本発明の場合には、興味のある非可逆的変形は、入力数値とほぼ同じだけの可能な出力数値を持つ。非可逆的変形は、（例えば、512ビット、または1024ビットのような）大きな入力フィールド、および出力フィールドを持たなければならない。そうすることにより、プロトコルのために必要なデータを一つのフィールド内に収容することができる。それ故、ゲームで使用するためのランダム・シードは、256ビットを必要とし、非可逆的変形への入力は、入力に追加のランダム・ビットを追加する：

【0069】

非可逆的変形への入力＝（データ・ストリーム、入力フィールドを「満たす」ためのランダム・データ・ストリーム）

【0070】

上記例の場合には、1024ビットの非可逆的変形および256ビットのシードである場合、「満たした」ランダム・データ・ストリームの長さは、768ビットである。非可逆的変形の一例としては、下記の形の関数がある：

$$\text{サンプル非可逆的変形}(x) = E(x) + x$$

【0071】

ここで、 $E(x)$ は、既知のキーを持つ優れた暗号化関数であり、 x は必要な長さの入力フィールドである。

【0072】

非可逆的変形は、キーを発生するためにも（下記参照）、ネットワーク・ゲーム実行取引処理プロトコルの秘密を保護し、確認できるようにするためにも使

用される。秘密保護プロセスは、保護されている2進表示で始まる：

秘密

秘密の非可逆的変形が、生成され、後の時点で、秘密を共有することになると思われる、他の当事者に供給される：

非可逆的変形（秘密）

秘密を公開する時がきた場合には、秘密を確認したいと願っている当事者に対して、秘密の決定を行った当事者により、「申し立てられた」秘密が供給される：

申し立てられた秘密

その後で、確認装置は、申し立てられた秘密の非可逆的変形を計算し、それを前に受信した秘密の非可逆的変形と比較する：

比較

非可逆的変形（申し立てられた秘密）

と、

前に受信した非可逆的変形（秘密）との比較

彼らが一致した場合には、秘密が公開され、秘密の決定に不公正な行為がないことが確認される。そうでない場合には、適当な他の手段をとることができる。非可逆的変形の特性のために、他の秘密は、受信した秘密を生成することはできなかったし、受信側は公開されるまで、その実際の秘密を再構成することができない。

【0073】

3. 4. 3 署名およびハッシュ機能

署名は、一人の個人だけが、サインしたメッセージを生成することができたことを確実にするために使用される。署名は、二つの要素、すなわち、ハッシング機能と、公開キー暗号化機能の組合せである。

【0074】

ハッシング機能は、データのすべての任意の変数の長さのストリームを選択し、それを、通常、ハッシュ数値と呼ばれる（例えば、1024ビットのような）比較的小さな一定の大きさのデータ・ブロックにする。ハッシング機能は、ハッ

シング機能およびデータ・ストリームが分かれば、計算により、同じハッシュ数値を持つ他のデータ・ストリームを発生することができるという属性を持つ。この条件は、実際には、多くの場合、弱められ、同じハッシュ数値を持つ、制御可能な入力データ・ストリームを生成することができなくなる。ハッシュ値は、計算により、ハッシュ値の「辞書」を生成することができるように、十分大きいものでなければならない。それ故、8ビットのハッシュ値は、あまりにも非常に小さすぎる。何故なら、この実施形態の場合には、 2^{1024} の可能な数値に対して、256の可能なハッシュ値(2^8)しか存在しないからである。

【0075】

公開キー暗号化機能は、作成者だけが、確実にメッセージを生成し、サインすることができるようにするために使用される。公開キー暗号化は、非対称の数学的関数をベースとしている。これらの関数においては、公開（解読）キーおよび数学的関数を知っていても、（それは作成した人だけが知っている秘密として維持されている）暗号化キーを再構成することはできない。この技術の最も有名な例が、市販のリバストーシャミールーアデルマン（RSA）プロセスである。この秘密の暗号化キーは、メッセージに対するハッシュ値を暗号化するのに使用される。それにより、それに「サイン」が行われる：

署名（メッセージ）＝暗号化_{秘密キー}（ハッシュ（メッセージ））

その後で、メッセージの作成者は、下記のペアを送る：

メッセージ、署名（メッセージ）

このプロセスの確認は、公開キー解読機能および公開ハッシュ機能を使用する：

解読_{公開キー}署名（受信したメッセージ）

と、

ハッシュ（受信したメッセージ）

との比較

【0076】

比較して、両方が一致した場合には、疑わしいメッセージ作成者は、サイン入りメッセージを生成することができる。このプロセス上で、機能が保持されてい

る限り、公開キーを使用しないで、署名を含む確認を使用することができる。

【0077】

3. 4. 4 協力シード／乱数発生

協力シードまたは協力乱数発生プロセスにより、そのプロセスに対するどの当事者も予測したり、制御することができない乱数を発生することができる。このプロセスは、乱数を発生するために、または直接乱数を生成するため目的で、シードを生成するために使用することができる。このプロセスのこの説明は、複数の当事者を含むが、そのうちの一方の当事者は賭博場と呼ばれ、他の当事者は、ゲーム参加者（1）～ゲーム参加者（N）と呼ばれる。この場合、Nは0より大きい整数である。このプロセスは、上記の非可逆的変形を使用する。

最初に、賭博場は、乱数を生成する：

乱数（賭博場）

次に、賭博場は、上記乱数の非可逆的変形を計算し、それをゲーム参加者に送る：

非可逆的変形（乱数（賭博場））

各ゲーム参加者は、また乱数を計算する：

乱数（ゲーム参加者（1））、乱数（ゲーム参加者（2））、

乱数（ゲーム参加者（3））、．．．、乱数（ゲーム参加者（N））

その後で、ゲーム参加者は、その各乱数の非可逆的変形を賭博場に供給し、また相互間で供給する：

非可逆的変形（乱数（ゲーム参加者（1））、

非可逆的変形（乱数（ゲーム参加者（2））、

非可逆的変形（乱数（ゲーム参加者（3））、．．．、

非可逆的変形（乱数（ゲーム参加者（N））

すべての当事者は、これら非可逆的変形を受信し、その後で、ゲーム参加者は、その乱数を賭博場に供給し、また相互間で供給する：

乱数（ゲーム参加者（1））、乱数（ゲーム参加者（2））、

乱数（ゲーム参加者（3））、．．．、乱数（ゲーム参加者（N））

【0078】

その後で、賭博場は、協力乱数を発生するために、ゲーム参加者の乱数をそれ自身の乱数と組み合わせる。この機能は、「排他的OR」のような簡単なものであってもよい：

協力乱数サイン＝関数（乱数（賭博場）、
乱数（ゲーム参加者（1））、乱数（ゲーム参加者（2））、
乱数（ゲーム参加者（3））、．．．、乱数（ゲーム参加者（N））

不公正な行為のないことを立証できる分散型ゲーム実行システムにおいては、この協力乱数は、直ちに公開することもできるし、確認段階で公開することもできる。上記乱数が公開されるまで、その乱数は、ゲームを保護するために、ホスト・カジノにより保護されなければならない。前に記憶した賭博場乱数の構造を制御しなかったことを確認するために：

非可逆的変形（乱数（賭博場））

を、ゲームの確認中に受信した、申し立てられた乱数の非可逆的変形と比較することができる：

非可逆的変形（申し立てられた乱数（賭博場））

賭博場を除外することにより、直ちに使用するための乱数を生成することができる。この生成は、秘密の乱数情報が必要ない場合に使用することができる。それ故、大部分のカード・ゲームは、賭博場を必要とするが、クラップスのようなゲームは、賭博場を必要としない。

【0079】

4．結論、派生効果および本発明の範囲

本明細書に記載したプロセスは、デッキを積み上げたり、公正なダイスを使用したりして、賭博場が自分達に不公正な行為をしていないという確信をもって、個人がゲームをすることができる環境を作ることによって、インターネット・ゲームを行うことを可能にする際に、一意の役割を持つことができる。

【0080】

上記説明は多くの特性を持っているが、これらの特性は、本発明の範囲を制限するものであると見なすべきではなく、その好適な実施形態の一例であると見なすべきである。多くの他の方法が可能である。例えば、機密保護および普通の

ゲームの実行を改善するために、賭博場での生のゲームのために、これを使用すれば、本明細書に記載する基本的プロトコルおよびアイデアをすべての使用することができる。パソコンの代わりに、Xターミナル；ウェブTV、ホテル内、家庭内または飛行機内のターミナル、または、ゲーム参加者があるスロット・マシンから他のスロット・マシンへ、またはあるテーブルから他のテーブルへ移動した場合、カジノ自身の内に重要なログ情報を保持する単なるメモリ・カードである、クライアント・プラットフォームを使用する、他のアーキテクチャも考慮の対象になる。これらの「機能の充実していないクライアント」オプションは、ゲーム参加者と、（2節で）詳細に説明したクライアント機能の大部分をピックアップするカジノの間に、追加のプロセッサを必要とする。それ故、中間システムは、ゲーム参加者とカジノとの間でエージェントの働きをする。しかし、この中間システムは、必ずしも信頼できるものでなくてもよい。

【0081】

さらに、本明細書に記載する装置およびプロセスは、通信ネットワークを通して行われる、ゲーム以外の取引にも使用することができる。例えば、上記技術は、株式、流通および日用品取引のような分野でも使用することができる。これら分野においては、買い注文と売り注文を、同時に、秘密に、または同時かつ秘密に行わなければならない。秘密のまたは同時のゲーム参加者の決定能力は、この機能をサードパーティに使用することができる。この場合、ゲームの規則は、特定のマーケット・タイプに対する売／買契約になる。本発明を使用すれば、ナスダックのような分散型マーケットを、ニューヨーク証券取引所で行われる公開オークション、すなわち、よりよい効率で値段を決めるマーケット機構と、同じタイプのものとすることができる。この技術を使用すれば、買い手および売り手は、人間のブローカを通さなくても交渉することができ、（お客の注文がないのに売り買いを行うような）ブローカの不正を防止することができる。これらの秘密のおよび同時の決定機能は、秘密性および同時性が重要な一般オークションおよび契約交渉のために役に立つ。

【0082】

選挙および投票は、選挙が終了するまで、投票内容を秘密にしたまま投票をす

ることができるようにする、秘密の決定機構を使用して実行することができ、人びとに投票させないようにする出口投票に関するいくつかの問題を軽減する。サンプルの他のメンバの偏向を最も少なくするように、秘密投票を保持することができる、投票は有利になる。

【0083】

モデル化、シミュレーション、電子商取引、または任意のタイプの取引システムのような他の用途も、本発明の機能により有利になる。モデル化の例の場合、ゲームの規則の代わりに、一組のヒューリスティック規則、神経ネット、ファジイ論理アルゴリズム、推理エンジン、または他の技術のようなモデル・エンジンが使用される。取引システムの場合には、ゲームの規則の代わりに、取引論理が使用される。従って、添付の特許請求の範囲は、上記の特定のゲーム実行の実施形態により制限されるものではなく、添付の特許請求の範囲およびそれに相当するものにより決定することができる。

【図面の簡単な説明】

【図1】

一般的なゲーム参加者／ゲーム・アーキテクチャ、すなわち、ゲームおよびカジノまたは「賭博場」の一般的な枠組みである。

【図2】

ゲーム参加者／ホスト・カジノ・ミドルウェア・アーキテクチャの図、すなわち、本発明の重要素子の関係、クライアントーサーバの関係を示す図である。

【図3】

一般的な物理的アーキテクチャの図、すなわち、本発明の通常の物理的構成部材およびそれらの関係を示す図である。

【図4】

ホスト・カジノ機能アーキテクチャの図、すなわち、ホスト・カジノの機能素子を示す図である。

【図5】

ホスト・カジノの物理的アーキテクチャの図、すなわち、ホスト・カジノの物理的素子およびそれらの関係を示す図である。

【図6】

ゲーム参加者システムの機能アーキテクチャの図、すなわち、ゲーム参加者システムの機能素子を示す図である。

【図7】

ゲーム参加者システムの物理的アーキテクチャの図、すなわち、ゲーム参加者システムの物理的素子およびそれらの関係を示す図である。

【図8】

トップ・レベルのプロセスの関係の図、すなわち、種々のトップ・レベルのプロセスの関係を示す図である。

【図9】

トップ・レベルの機能の流れを示す図、すなわち、本発明の動作中に使用されるトップ・レベルの流れを示す図である。

【図10】

キーの図、すなわち、フローチャートで使用される素子を示す図である。

【図11】

ゲーム参加者登録フローチャート、すなわち、ゲーム参加者登録プロセスを示す図である。

【図12】

ゲーム設定フローチャート、すなわち、ゲーム設定プロセスの流れを示す図である。

【図13】

ゲーム設定フローチャート、すなわち、ゲーム設定プロセスの流れを示す図である。

【図14】

ゲーム実行のフローチャート、すなわち、ゲーム実行プロセスの流れを示す図である。

【図15】

ゲーム実行のフローチャート、すなわち、ゲーム実行プロセスの流れを示す図である。

【図16】

ゲーム確認フローチャート、すなわち、ゲーム確認プロセスを示す図である。

【図17】

ゲーム確認フローチャート、すなわち、ゲーム確認プロセスを示す図である。

【図18】

ホストゲーム参加者間の取引きのフローチャート、すなわち、ホストゲーム参加者間の取引きのプロセスを示す図である。

【図19】

機密保護ホストゲーム参加者間の通信フローチャート、すなわち、機密保護ホストゲーム参加者間の通信プロセスを示す図である。

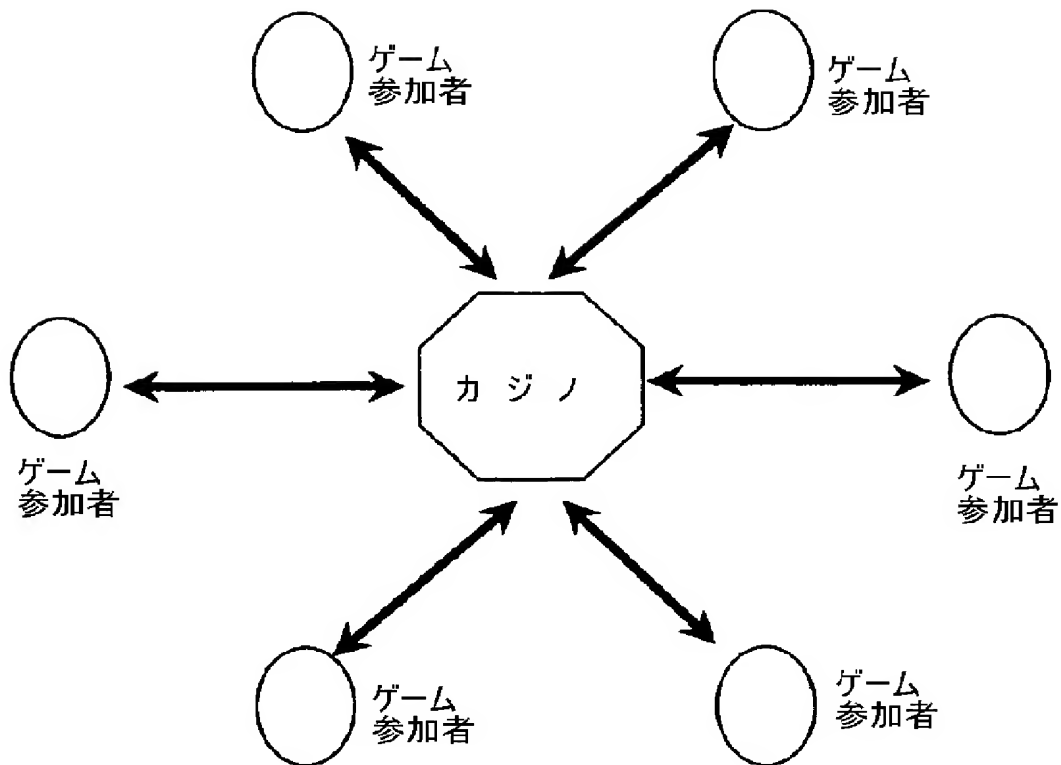
【図20】

プロトコルおよびパケットの図、すなわち、ネットワークを通してプロトコルがどのように送信されるのか、（また通常、カプセル化、トンネル化とも呼ばれる）プロトコルが、どのようにして相互に入れ子状態になるのかを示す図である。

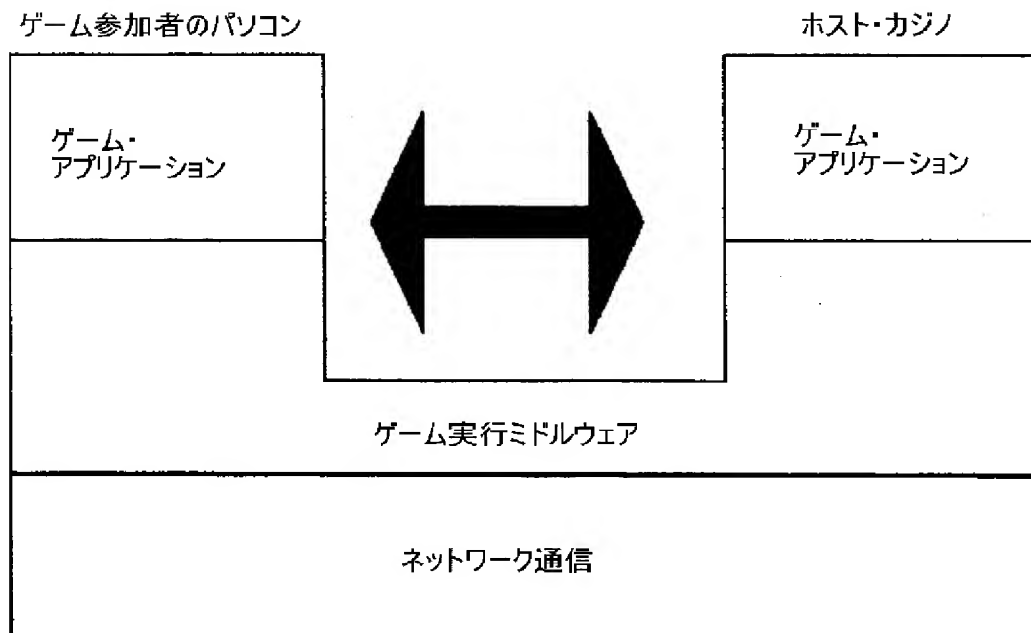
【図21】

一般的ゲーム・アーキテクチャの図、すなわち、ゲームの素子、すなわち、イベント、決定、規則、環境、データ記憶および状態を示す図である。

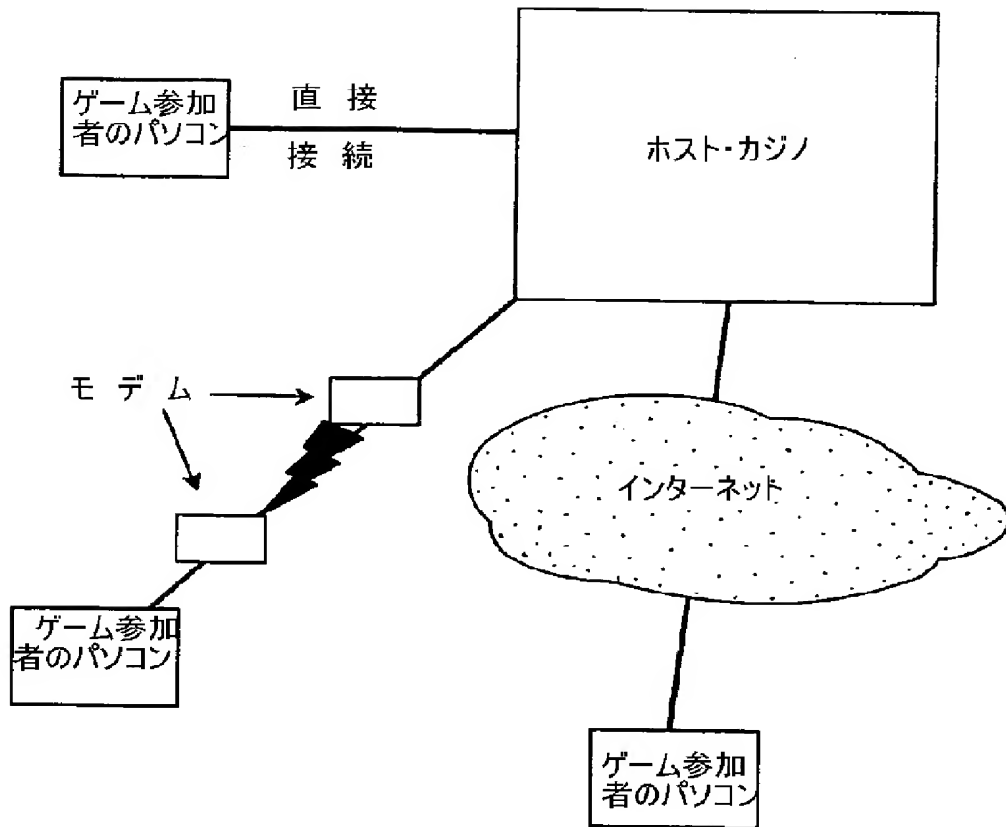
【図1】



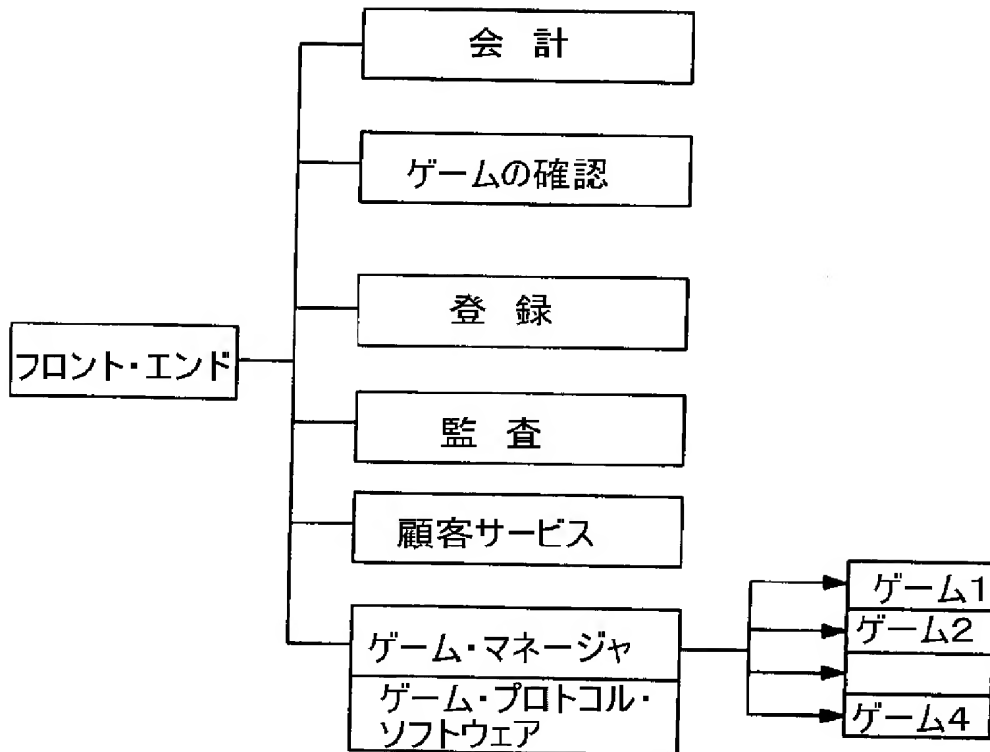
【図2】



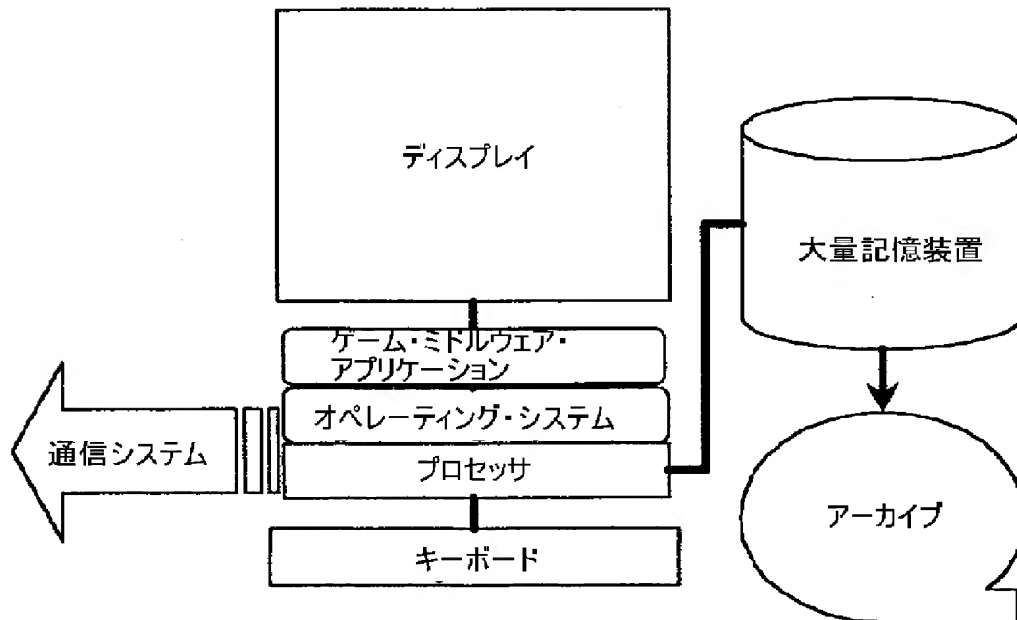
【図3】



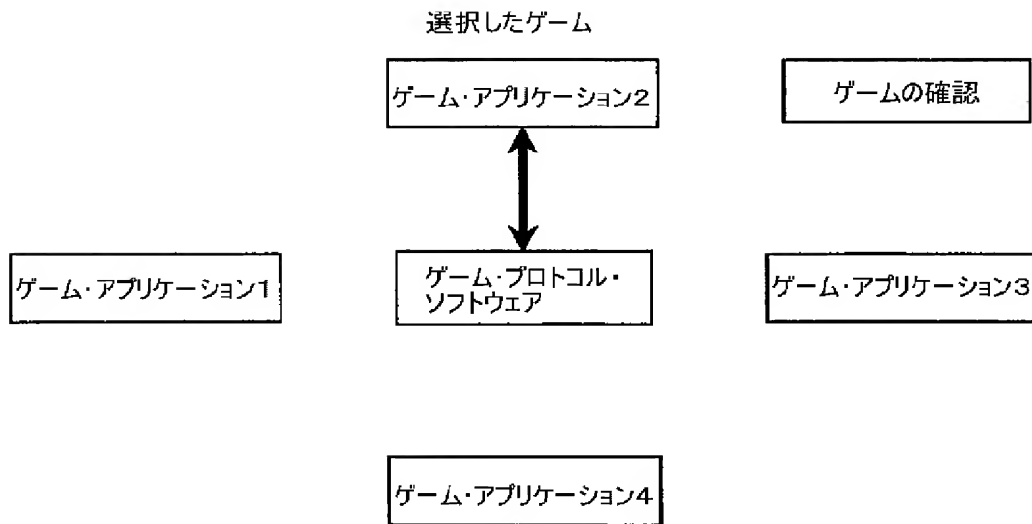
【図4】



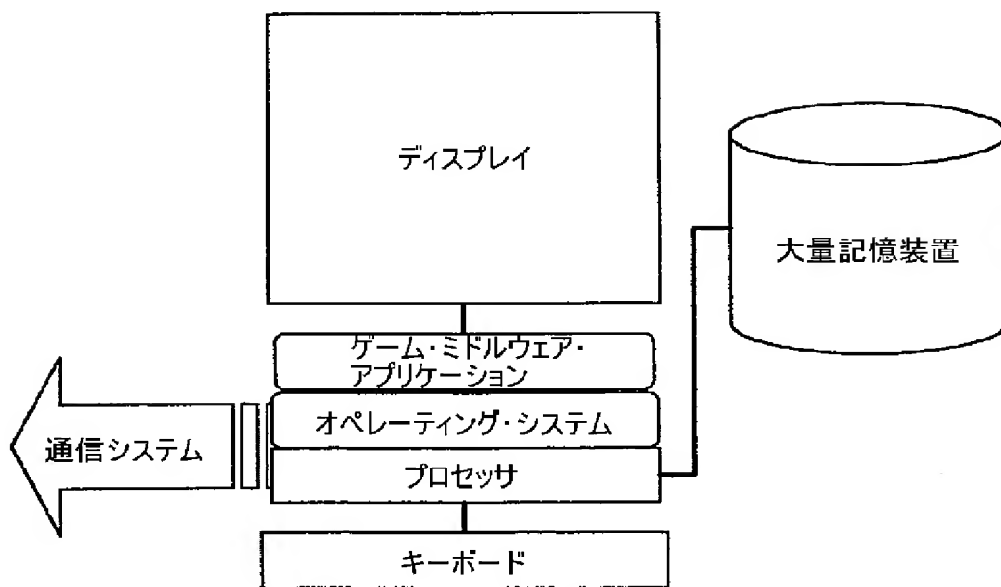
【図5】



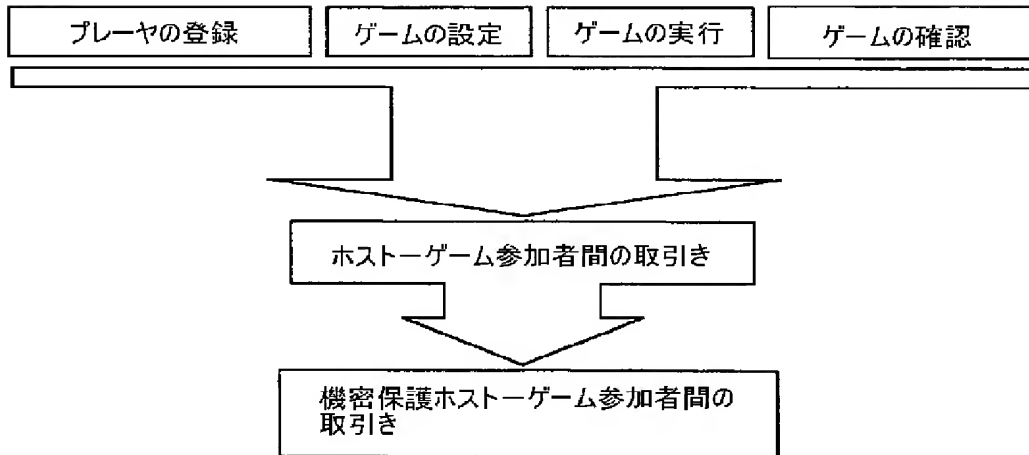
【図 6】



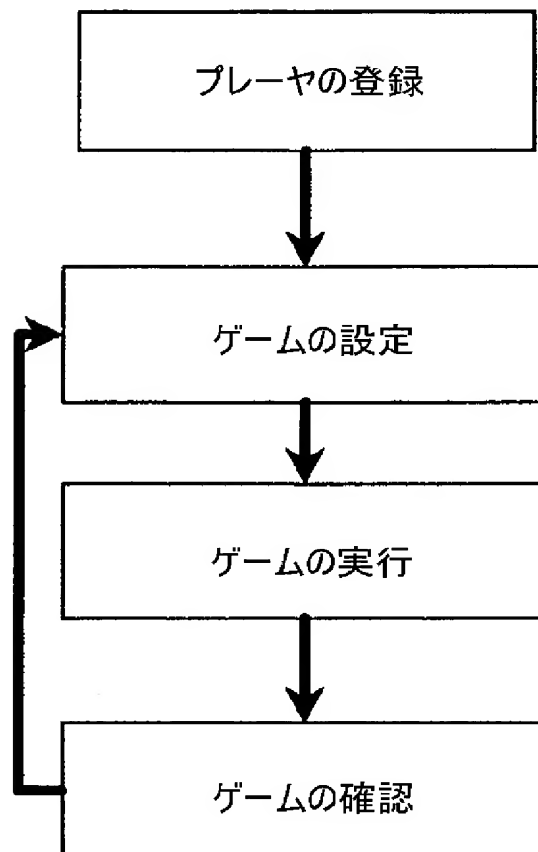
【図 7】



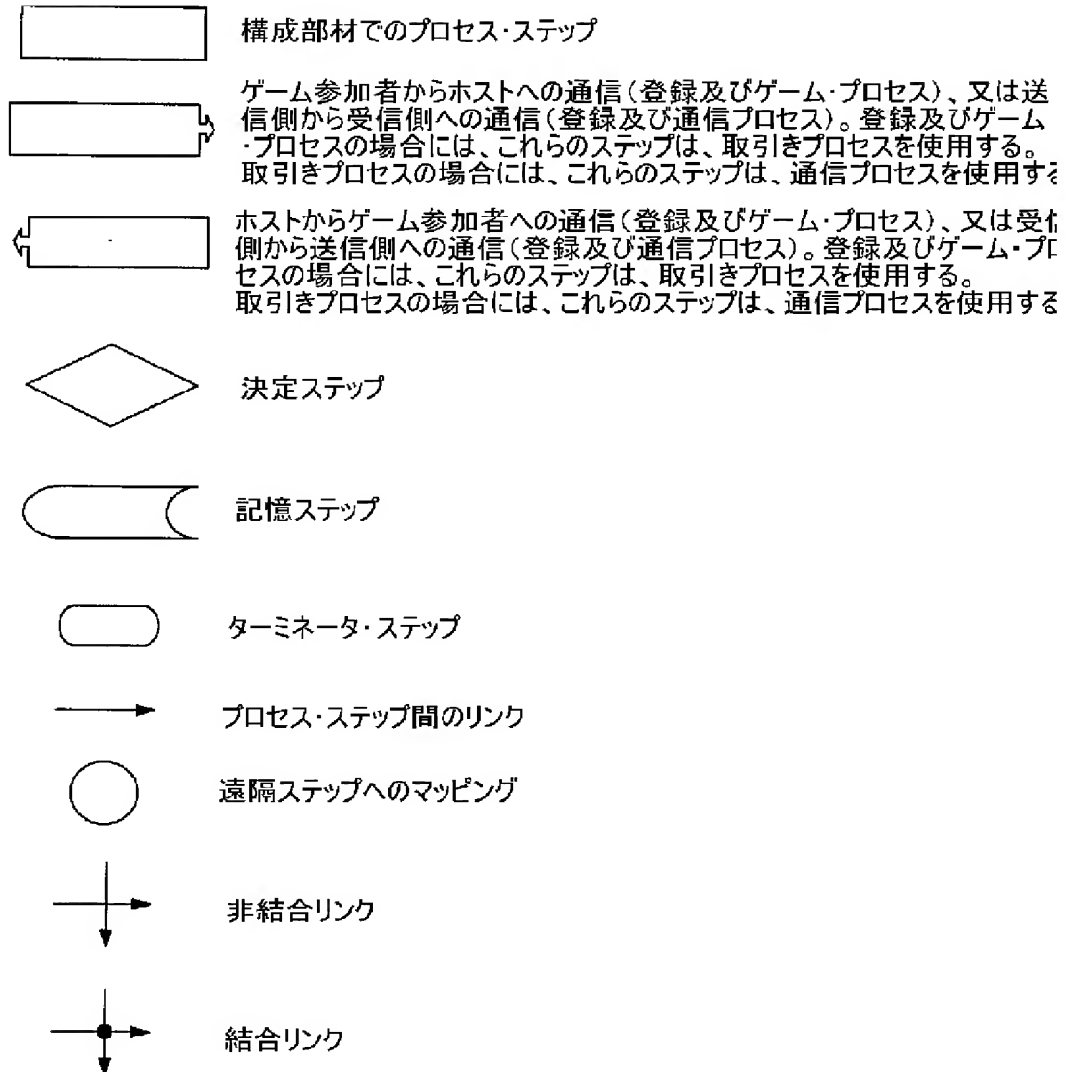
【図 8】



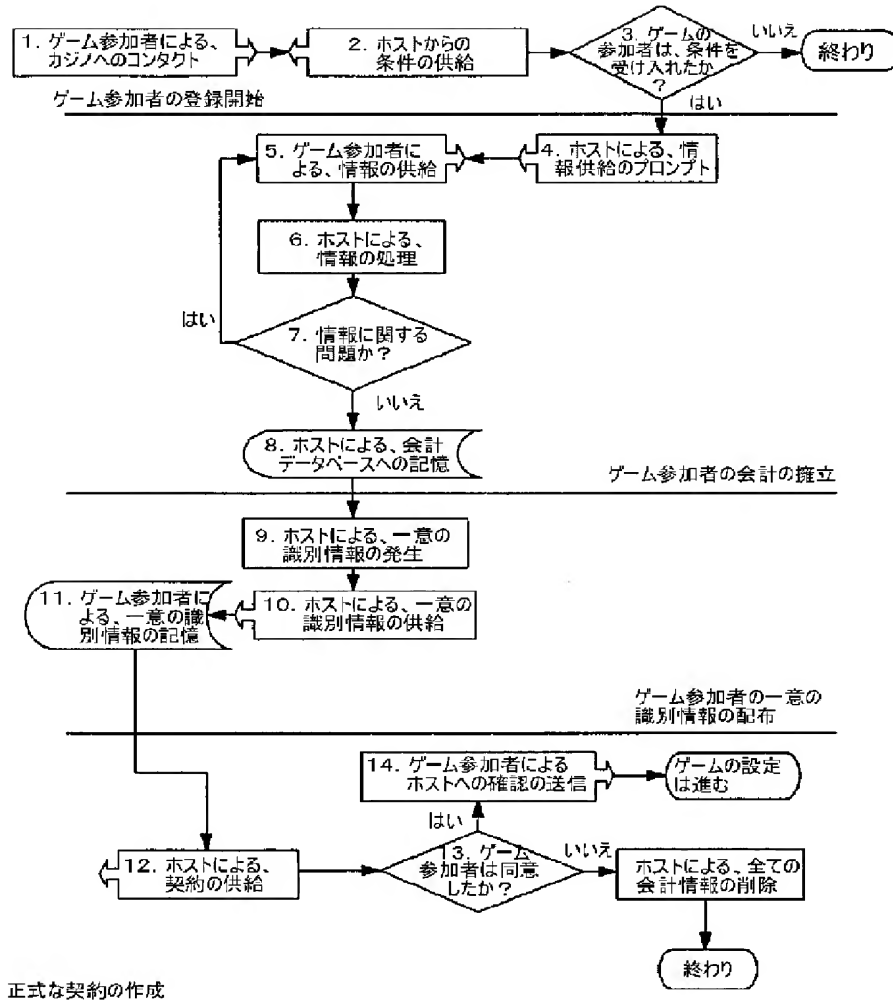
【図 9】



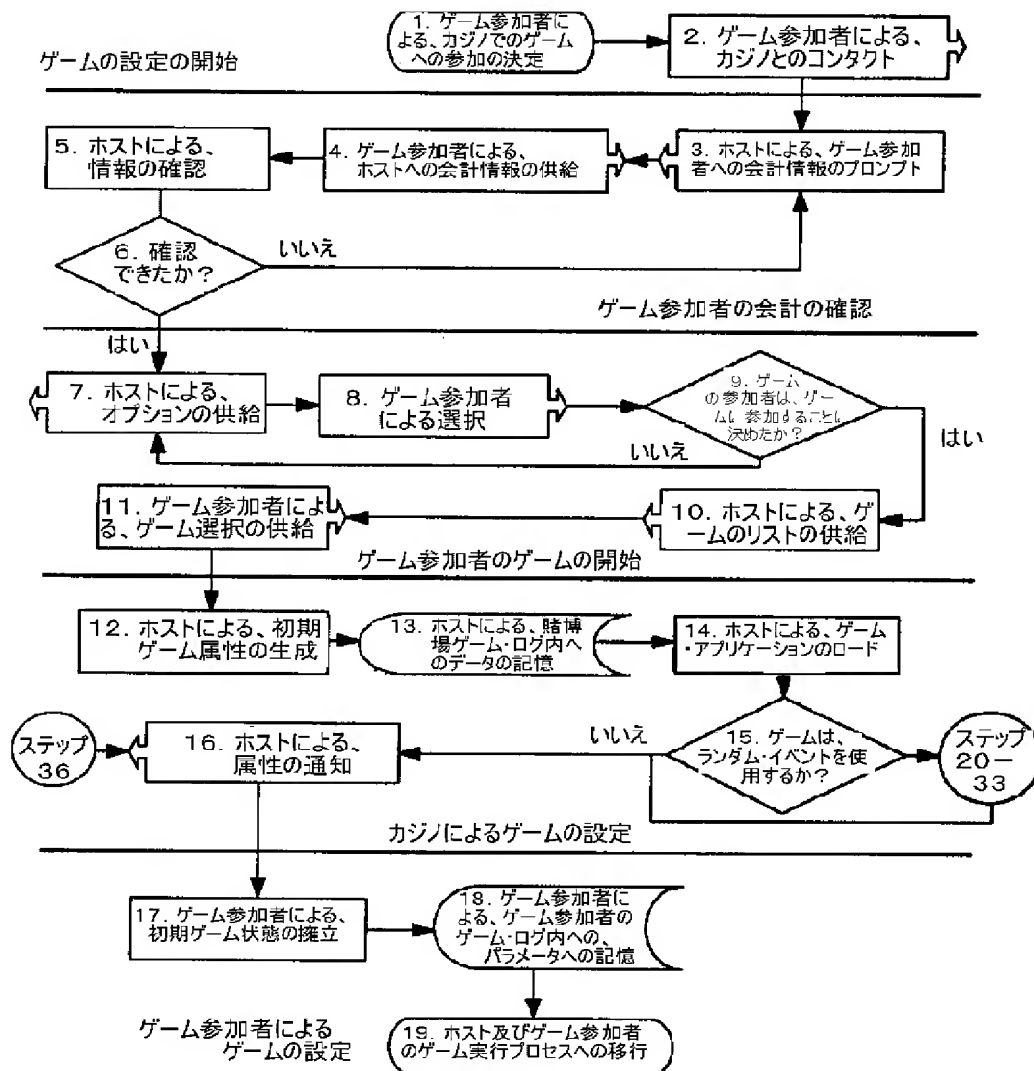
【図10】



【図11】

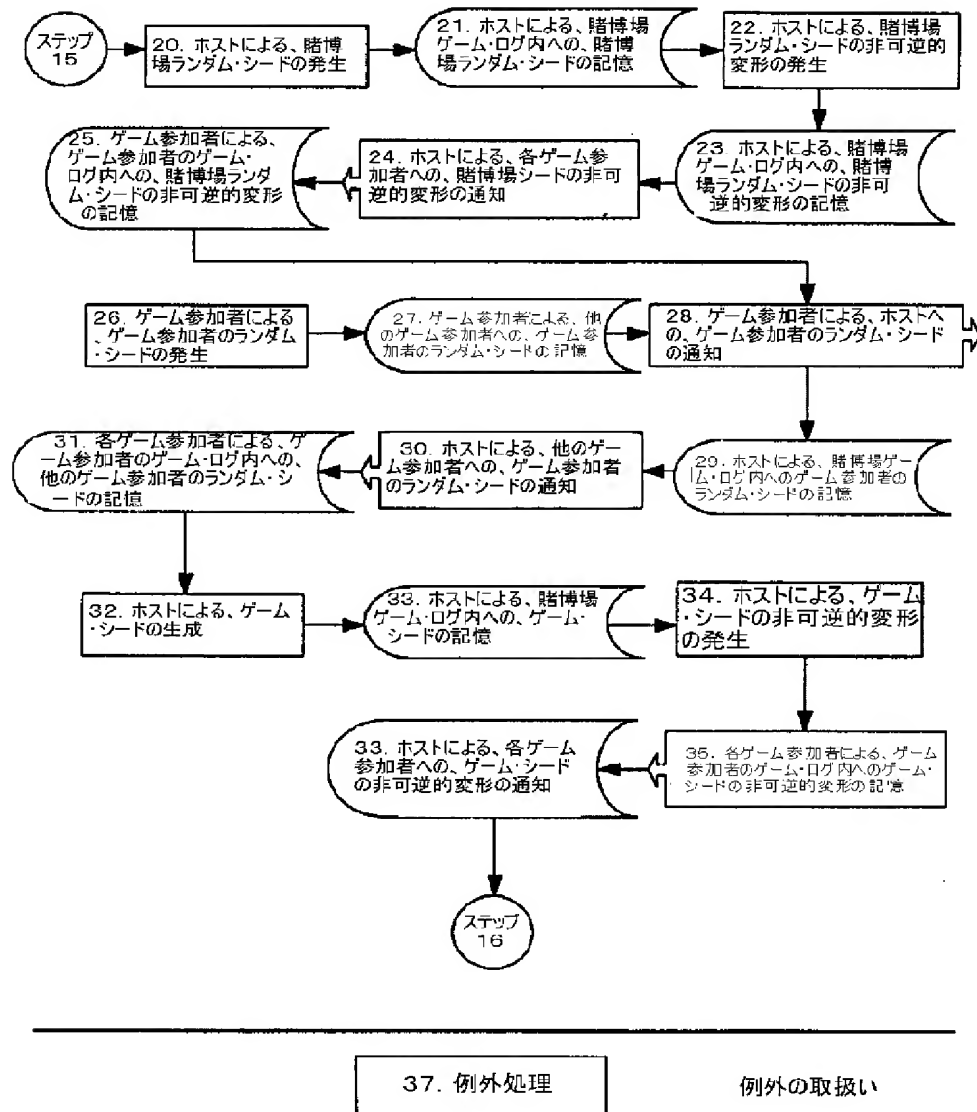


【図12】

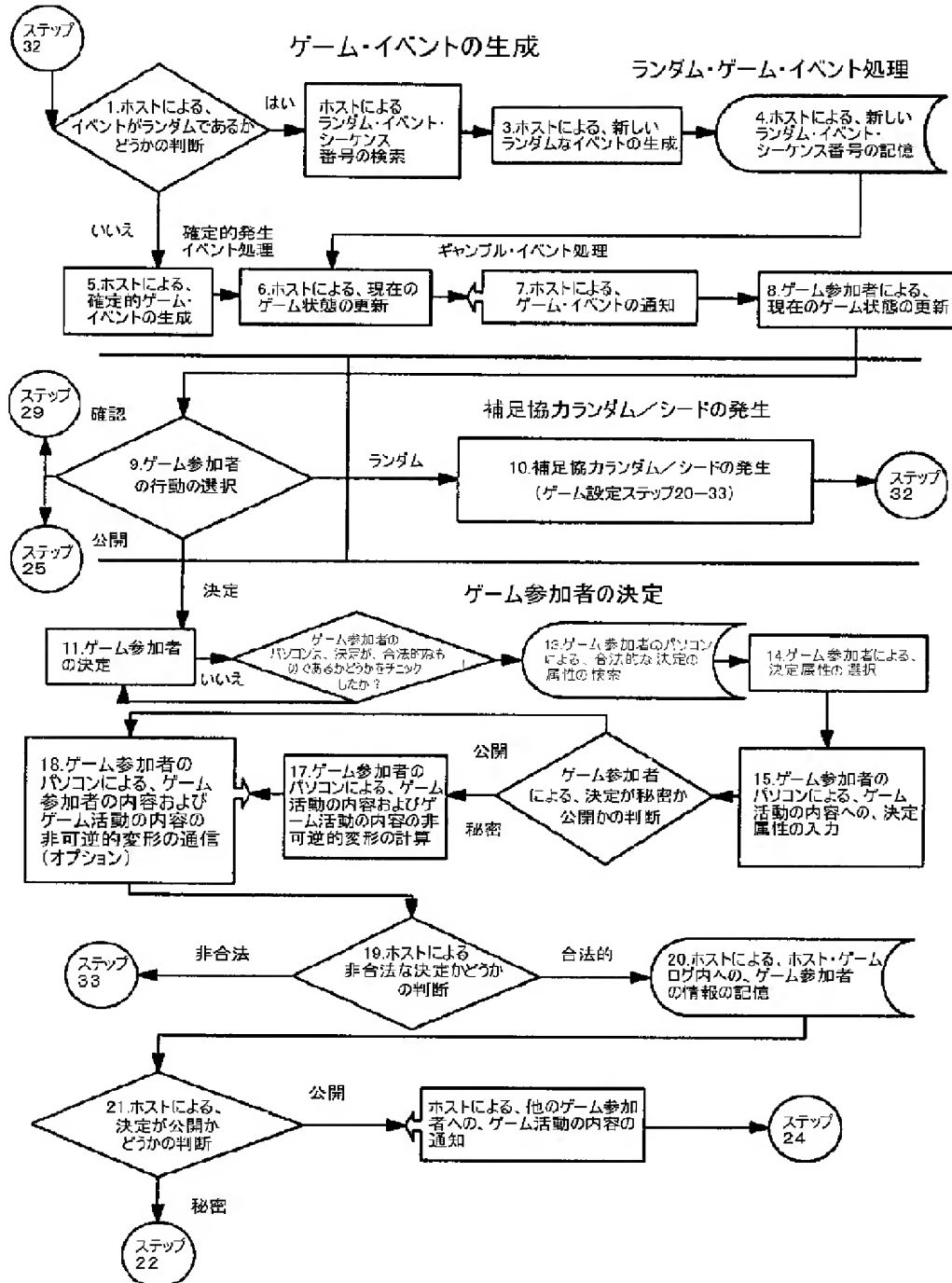


【図13】

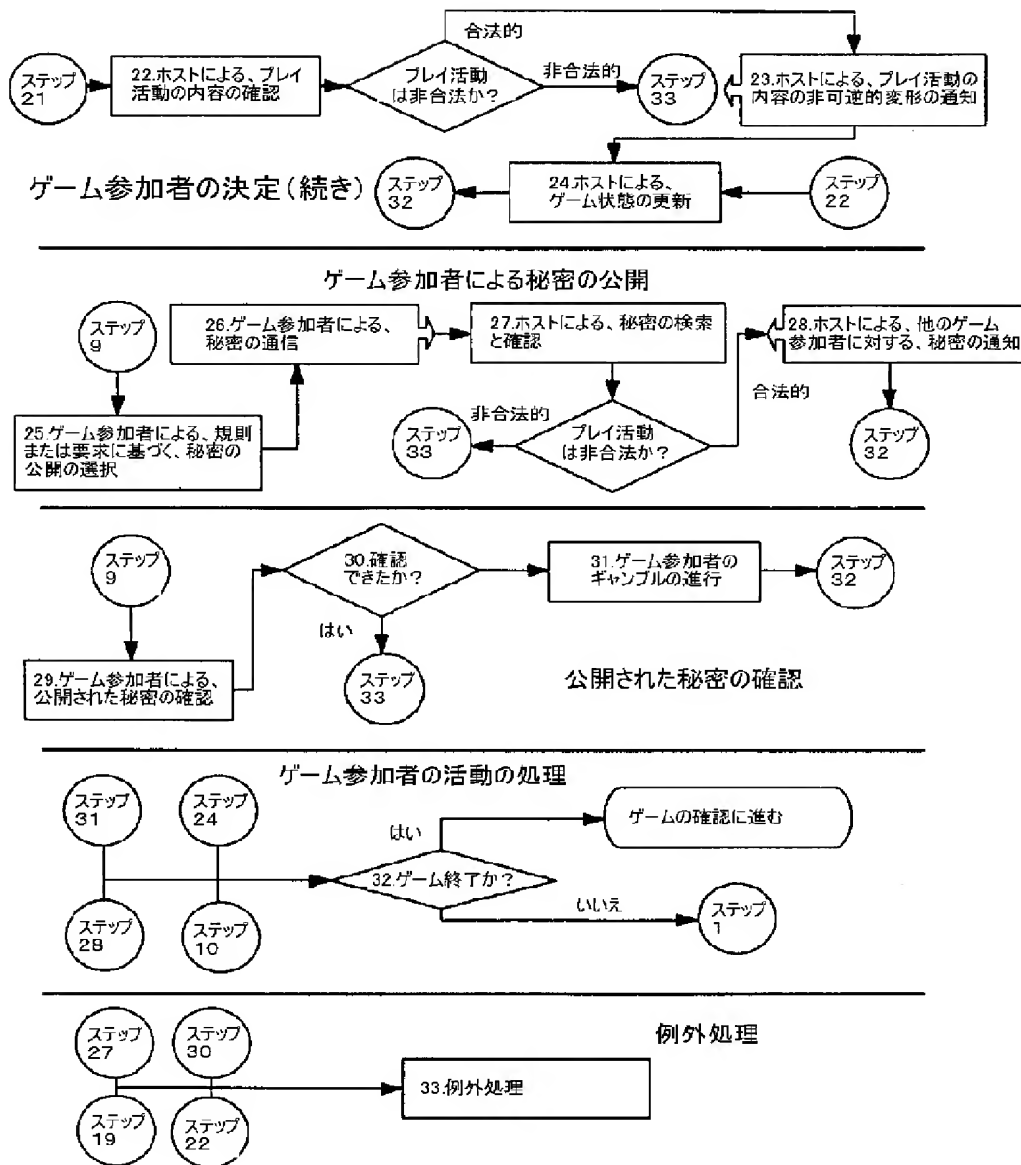
協カゲーム・シード発生



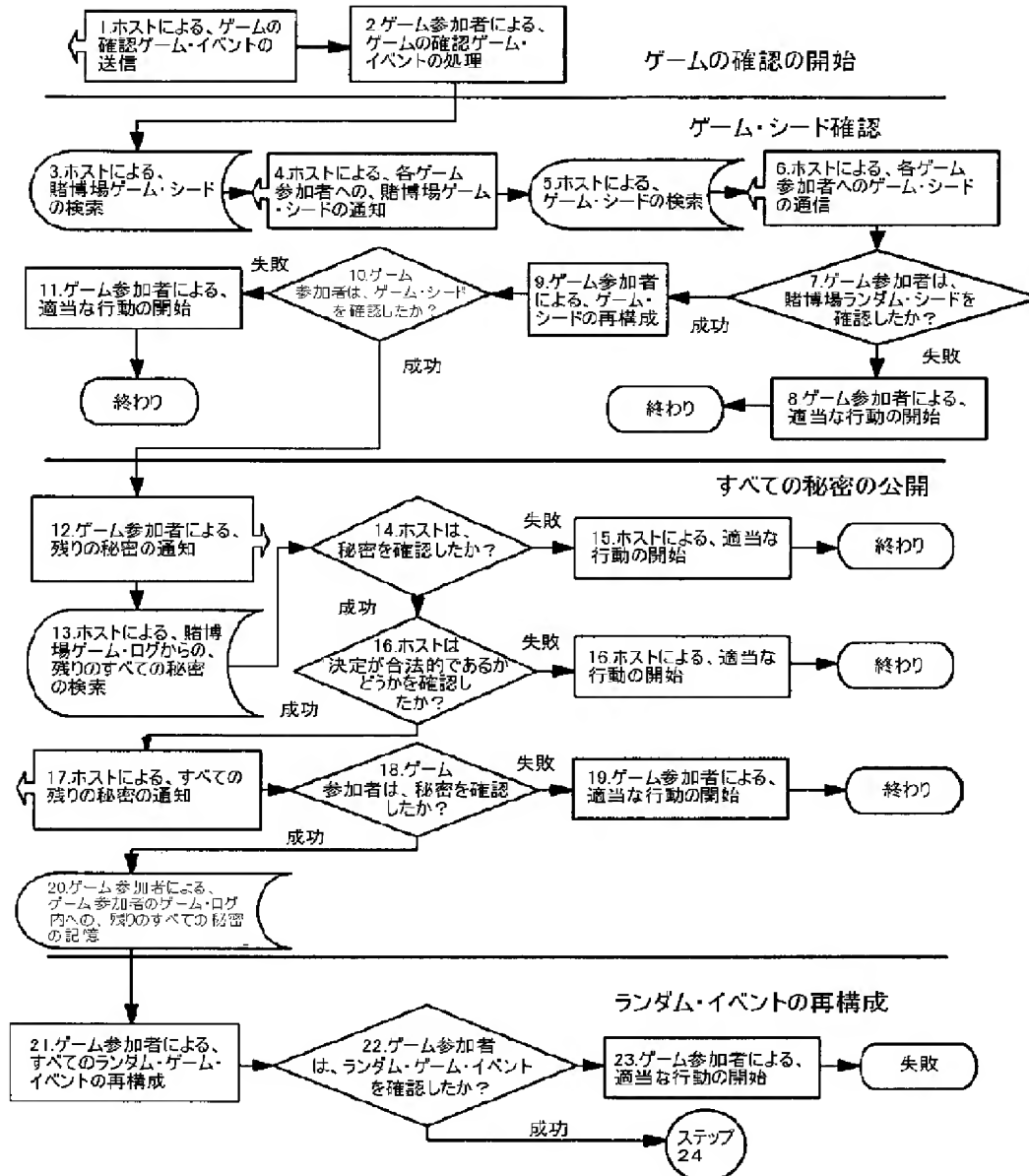
【图 1-4】



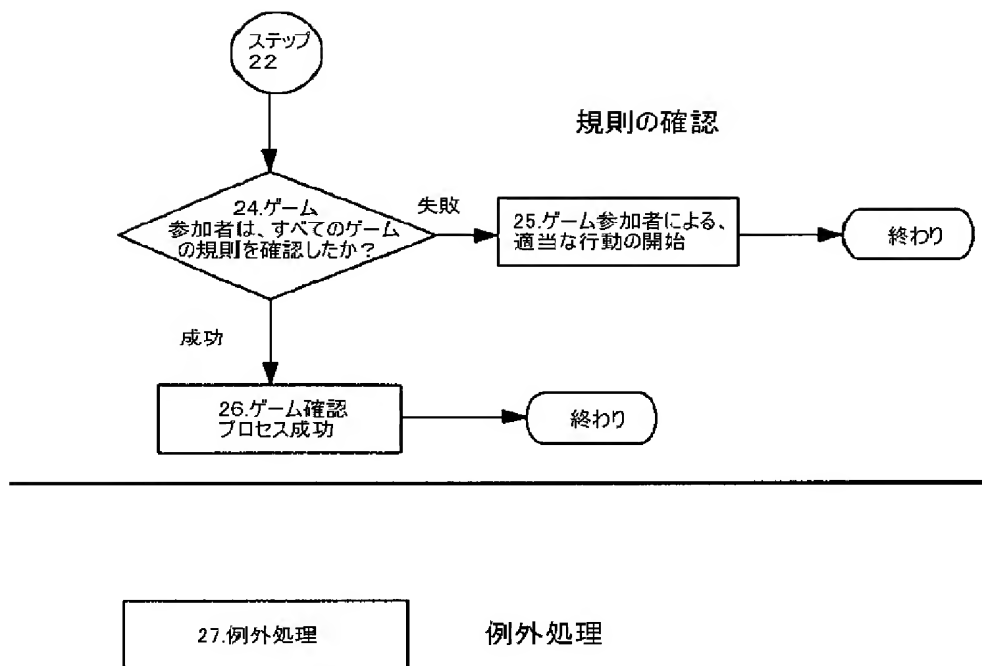
【図15】



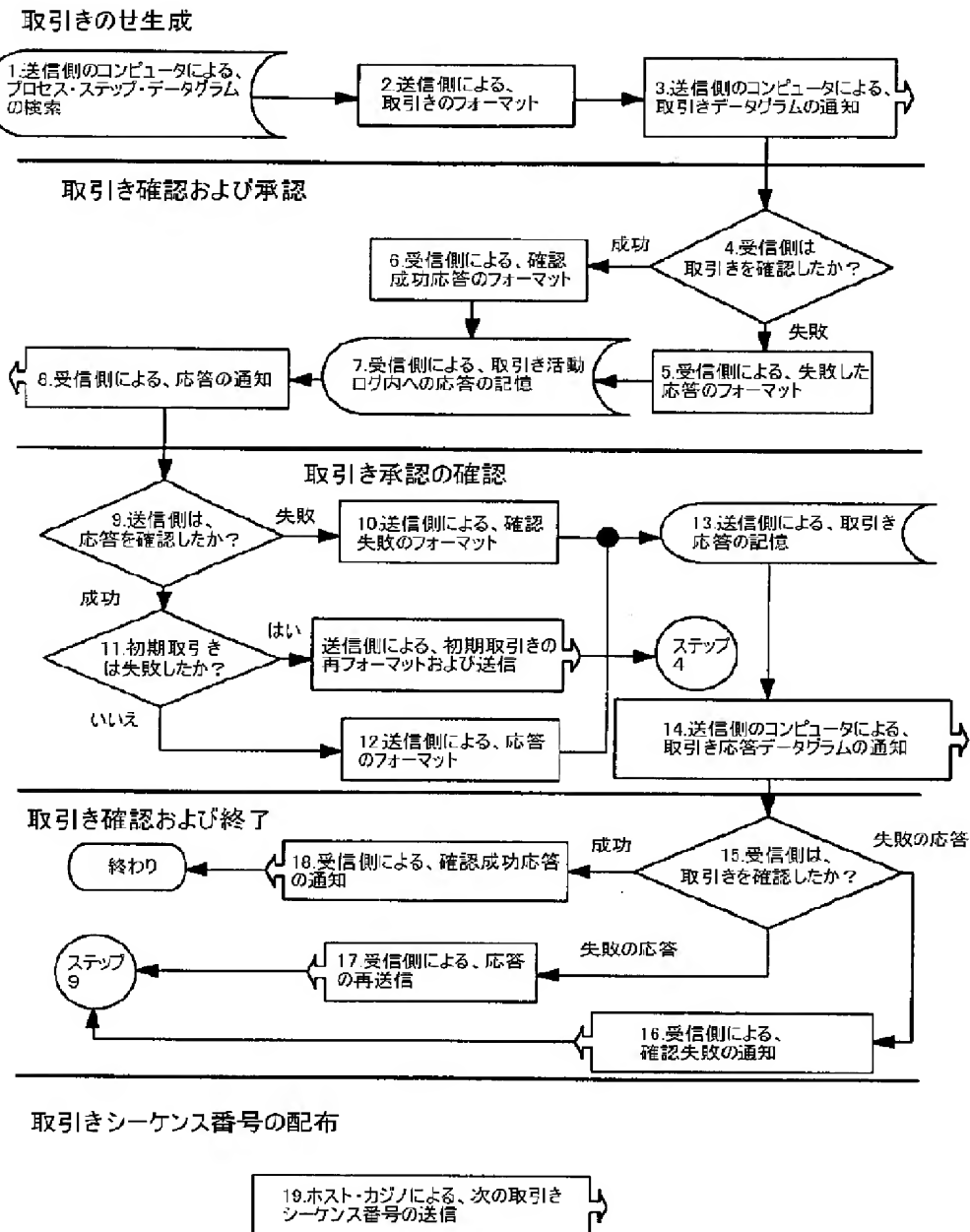
【図16】



【図17】

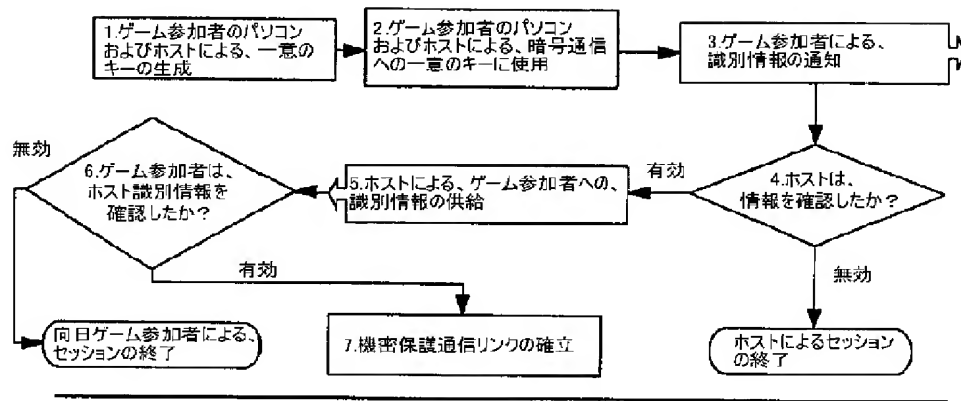


【図18】

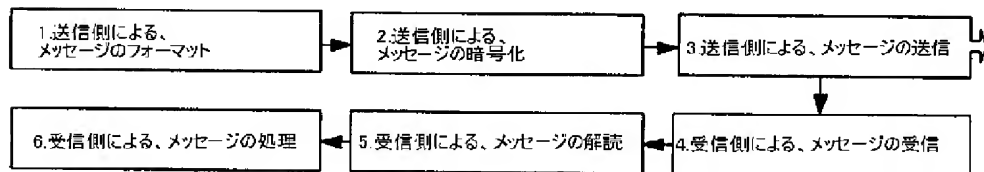


【図19】

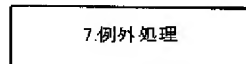
カジノにおけるセッションの開始



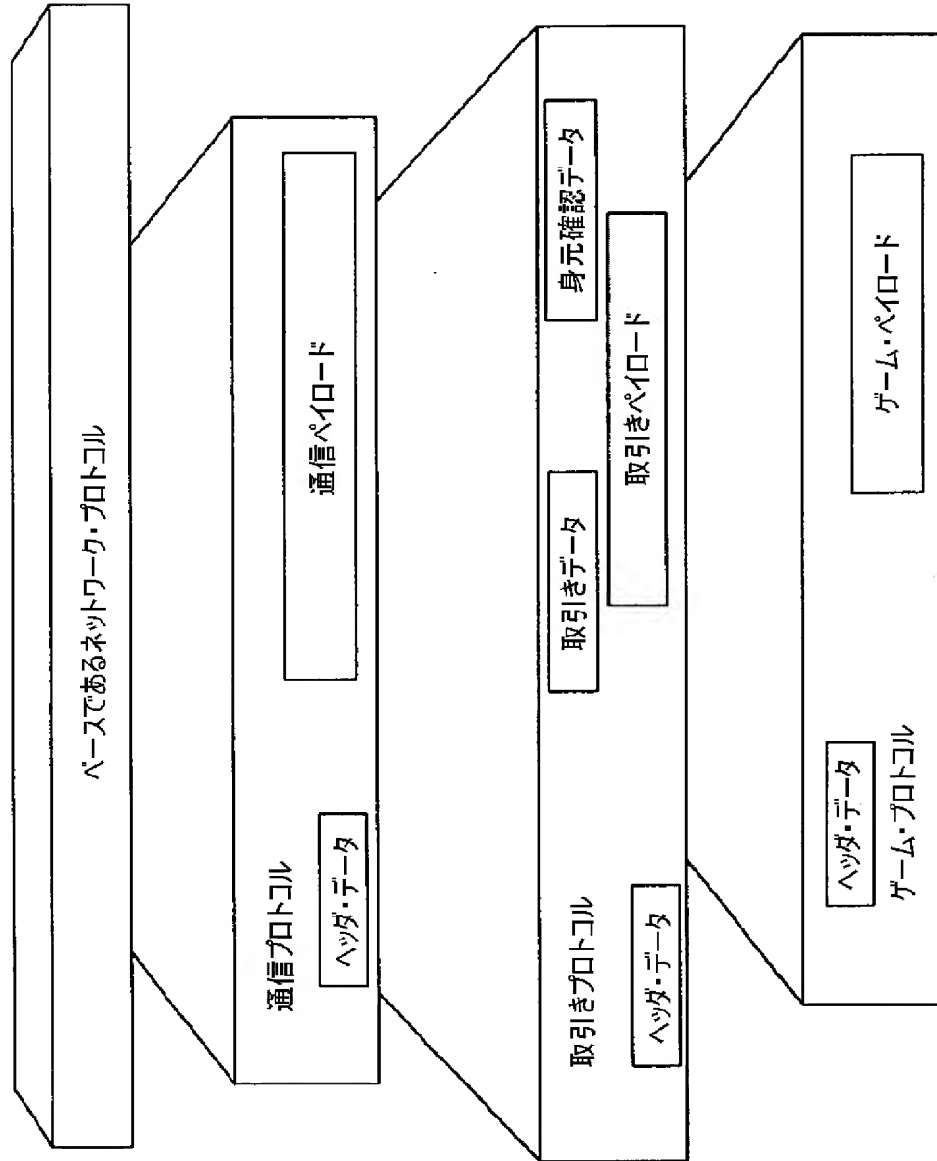
ゲーム参加者とホスト・カジノとの間の確認通信の場合



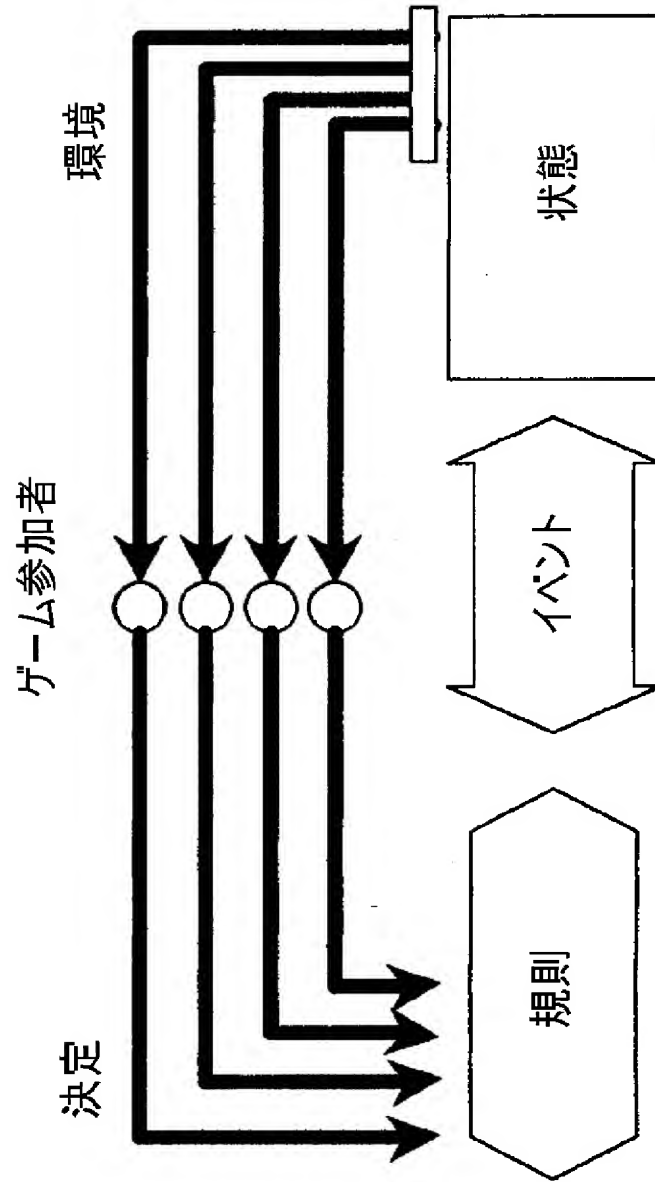
例外処理



【図20】



【図 2 1】



【手続補正書】

【提出日】 平成12年4月12日 (2000. 4. 12)

【手続補正1】

【補正対象書類名】 明細書

【補正対象項目名】 特許請求の範囲

【補正方法】 変更

【補正内容】

【特許請求の範囲】

【請求項1】 通信ネットワークを通して、公正なゲーム進行手続を確保するための装置であって、

ゲーム・シードを発生するためのホスト・プロセッサであり、衛星プロセッサからゲーム入力を受信し、前記ゲーム入力、ゲーム・シード、および予め定めたゲームの規則から、ゲームの結果を発生し、前記ゲーム・シードおよび前記ゲームの結果を前記衛星プロセッサに送信するホスト・プロセッサと、

前記通信ネットワークを通して、前記ゲーム入力を供給し、前記ホスト・プロセッサから、前記ゲーム・シードおよび前記ゲームの結果を受信し、(i) 前記ゲーム入力、前記ゲーム・シード、および前記の予め定めゲームの規則に基づいて、ゲームの結果を発生し、(ii) 前記の発生したゲームの結果を、前記の受信したゲームの結果とを比較するための衛星プロセッサとを備える装置。

【請求項2】 請求項1に記載の装置において、前記衛星プロセッサが、前記ゲーム・シードを発生するために、前記ホスト・プロセッサが使用する衛星乱数を供給する装置。

【請求項3】 請求項1に記載の装置において、前記ホスト・プロセッサが、前記ゲーム・シードを発生するために、前記ホスト・プロセッサが使用するホスト乱数を発生する装置。

【請求項4】 請求項3に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数からホスト変形を発生し、前記ホスト変形を前記衛星プロセッサに供給する装置。

【請求項5】 請求項4に記載の装置において、前記ホスト・プロセッサが

、前記衛星プロセッサに、前記ホスト乱数を供給し、前記衛星プロセッサが、前記ホスト変形が供給したホスト乱数から発生したものであることを確認するために、前記ホスト乱数および前記ホスト変形を使用する装置。

【請求項6】 請求項5に記載の装置において、前記衛星プロセッサが、前記ホスト乱数から前記ゲーム・シードを発生する装置。

【請求項7】 請求項4に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数の非可逆的変形から前記ホスト乱数を計算する装置。

【請求項8】 通信ネットワークを通して、合作のランダム出力を生成するための装置であって、

ホスト乱数を発生するためのホスト・プロセッサであり、衛星プロセッサから衛星乱数を受信し、前記衛星乱数、および前記ホスト乱数に基づいて、協力ランダム出力を発生するホスト・プロセッサと、

前記衛星乱数を発生し、前記通信ネットワークを通して、前記衛星乱数を前記ホスト・プロセッサに供給するための衛星プロセッサとを備える装置。

【請求項9】 請求項8に記載の装置において、前記ホスト・プロセッサが、ゲーム・シードを発生するために、前記協力ランダム出力を使用する装置。

【請求項10】 請求項8に記載の装置において、前記ホスト・プロセッサが、前記通信ネットワークを通して、前記衛星プロセッサに前記ホスト乱数を供給し、前記衛星プロセッサが、前記協力ランダム出力を確認するために、前記衛星乱数および前記ホスト乱数を使用する装置。

【請求項11】 請求項8に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数からホスト変形を発生し、前記ホスト変形を、前記通信ネットワークを通して、前記衛星プロセッサに供給し、前記衛星プロセッサが、前記ホスト乱数を確認するために、前記ホスト変形および前記ホスト乱数を使用する装置。

【請求項12】 請求項11に記載の装置において、前記ホスト・プロセッサが、前記ホスト乱数の非可逆的変形から前記ホスト変形を計算する装置。

【請求項13】 通信ネットワークを通して、取引を確認するための装置であって、

(i) 前記通信ネットワークを通して、第二プロセッサから第二のプロセッサ入力変形を受信し、

(ii) 任意の ゲーム入力が発生し、

(iii) 前記任意の ゲーム入力から第一のプロセッサ入力変形を計算し、

(iv) 前記第一のプロセッサの入力変形を、前記通信ネットワークを通して、第二のプロセッサに送り、

(v) (i) および (iv) ステップの後で、前記通信ネットワークを通して、前記任意のゲーム入力を前記第二のプロセッサに送り、

(vi) 前記通信ネットワークを通して、前記第二のプロセッサから任意のゲーム入力を受信し、

(vii) (vi) ステップの後で、前記第二のプロセッサの入力変形を、(v) ステップで受信した前記任意のゲーム入力と比較するための第一プロセッサと、

(i) 前記通信ネットワークを通して、前記第一のプロセッサから前記第一のプロセッサの入力変形を受信し、

(ii) 第二の任意のゲーム入力が発生し、

(iii) 前記の任意の決定入力から前記第二のプロセッサの入力変形を計算し、

(iv) 前記通信ネットワークを通して、前記の第二のプロセッサの入力変形を前記の第一のプロセッサに送り、

(v) (i) および (iv) ステップの後で、前記通信ネットワークを通して、前記の第二の任意のゲーム入力を前記の第一のプロセッサに送り、

(vi) 前記通信ネットワークを通して、前記の第一のプロセッサから前記の任意の決定入力を受信し、

(vii) (vi) ステップの後で、前記第一のプロセッサの入力変形を、(v) ステップで受信した前記任意の決定入力と比較するための第二のプロセッサとを備える装置。

【請求項14】 請求項13に記載の装置において、前記第一のプロセッサの入力変形および前記第二のプロセッサの入力変形が、前記決定入力の非可逆的

変形に基づくものである装置。

【請求項15】 通信ネットワークを通して、公正なゲーム進行手続を確保するための装置であって、

(i) 通信ネットワークを通して、二つの各衛星プロセッサから任意のゲーム入力を受信し、

(ii) 各衛星プロセッサに対する前記任意のゲーム入力に対応するデータを前記の他の衛星プロセッサに送り、

(iii) 前記の二つのプロセッサからの任意のゲーム入力、および予め定めたゲームの規則を使用して、ゲームの結果を作成し、

(iv) 前記通信ネットワークを通して、前記のゲームの結果を前記衛星プロセッサに供給し、

(v) (iv) ステップの後で、前記通信ネットワークを通して、すべての任意のゲーム入力を各衛星プロセッサに供給するためのホスト・プロセッサと、

(i) 任意のゲーム入力を決定し、

(ii) 前記通信ネットワークを通して、前記の任意のゲーム入力を前記ホスト・プロセッサに供給し、

(iii) 前記通信ネットワークを通して、前記のゲームの結果を前記ホスト・プロセッサから受信し、

(iv) 前記通信ネットワークを通して、前記ホスト・プロセッサから前記のゲームの結果を受信し、

(v) 前記のゲームの結果を記憶し、

(vi) 前記通信ネットワークを通して、前記ホスト・プロセッサから前記の他の衛星プロセッサのゲーム入力を受信し、

(vii) 前記の他の衛星プロセッサのゲーム入力を記憶し、

(viii) (a) 前記の他の衛星プロセッサの任意のゲーム入力と、前記の記憶した任意のゲーム入力と、前記記憶した予め定めたゲームの規則からゲームの結果を発生し、

(b) 前記の発生したゲームの結果を、前記の記憶したゲームの結果と比較することにより、前記ゲーム実行取引を確認するための二つの各衛星プロセッサ

を備える装置。

【請求項16】 請求項15に記載の装置において、前記ホスト・プロセッサが、さらに、

前記各衛星プロセッサのゲーム入力から発生したデータを受信し、

前記通信ネットワークを通して、前記各衛星プロセッサからの前記発生データを前記の他の衛星プロセッサに転送し、

また、各衛星プロセッサが、さらに、

(i) 前記ホスト・プロセッサに前記ゲーム入力から発生したデータを供給し、

(ii) 前記の他の衛星プロセッサからの前記ゲーム入力からの発生データを受信し、

(iii) 前記の他の衛星プロセッサから前記ゲーム入力を受信した後で、前記ゲーム入力に対応するデータを計算し、前記出力を計算したデータと呼び、

(iv) (iii) ステップの後で、前記ゲーム入力から計算したデータと、前記ゲーム入力に対応する前記の前に受信したデータとを比較する装置。

【請求項17】 請求項15に記載の装置において、前記決定入力に対応する前記データが、前記決定入力の非可逆的変形から計算される装置。

【請求項18】 請求項15に記載の装置において、前記ホスト・プロセッサが、各衛星プロセッサに対する前記任意の決定入力に対応するデータを計算する装置。

【請求項19】 前記衛星プロセッサが、前記ホスト・プロセッサに乱数を供給し、

前記ホスト・プロセッサが、前記の受信した乱数に基づいて、ゲーム・シードを発生し、

前記衛星プロセッサが、前記ホスト・プロセッサにゲーム入力を供給し、

前記ホスト・プロセッサが、前記ゲーム入力、前記ゲーム・シード、および予め定めたゲームの規則に基づいて、ゲームの結果を発生し、

前記衛星プロセッサが、前記ホスト・プロセッサから、前記ゲーム・シードおよび前記のゲームの結果を受信し、

前記衛星プロセッサが、(i) 前記ゲーム入力、前記ゲーム・シードに対応する前記データ、および予め定めたゲームの規則に基づいて、ゲームの結果を発生し、(ii) 前記の発生したゲームの結果を、前記の受信したゲームの結果と比較することにより、前記取引きに不公正な行為がないことを確認し、これらのプロセスにより、通信ネットワークを通して、一つまたはそれ以上のコンピュータに、公正なゲーム進行手続を確保するためのプログラムを記憶するための記憶媒体。

【請求項20】 通信ネットワークを介して協同ランダム出力を生成するための装置であって、

ホスト乱数を発生するためのホストプロセッサを含み、該衛星プロセッサは、衛星プロセッサから衛星乱数を受信し該衛星乱数および該ホスト乱数に基づいて処理シードを発生し、該ホスト乱数から非可逆的変換を発生し、それを該衛星プロセッサから任意の処理入力を受信する前に該衛星プロセッサに提供し、および(i) 受信された任意の手続入力および(ii)該処理シードを用いて処理出力を決定することを特徴とする装置。

【請求項21】 通信にかかわる第1のプロセッサおよび第2のプロセッサを有する通信ネットワークを介してデータ処理を生成しおよび確認するための装置において、

該第1のプロセッサは、

(i) 該通信ネットワークを介して該第2のプロセッサから該第2のプロセッサデータ入力非可逆的変換を受信し、

(ii) 第1のプロセッサ任意データ入力を発生し、

(iii)該第1のプロセッサ任意データ入力から第1のプロセッサデータ入力非可逆的変換を計算し、

(iv) 該通信ネットワークを介して該第2のプロセッサに対して該第1のプロセッサデータ入力非可逆的変換を通信し、

(v) 上記ステップ(i)および(iv)の後で、該通信ネットワークを介して該第2のプロセッサに対して該第1の任意データ入力を通信し、

(vi) 該通信ネットワークを介して該第2のプロセッサから第2のプロセッサ

任意データ入力を受信し、

(vii)上記ステップ(vi)の後で、該第2のプロセッサ非可逆的変換を上記ステップ(vi)において受信された該第2のプロセッサ任意データ入力と比較することを特徴とする装置。

【請求項22】 通信にかかわる第1のプロセッサおよび第2のプロセッサを有する通信ネットワークを介してデータ処理を生成しおよび確認するための装置において、

該第2のプロセッサは、

(i) 該通信ネットワークを介して該第1のプロセッサから第1のプロセッサデータ入力非可逆的変換を受信し、

(ii) 第2のプロセッサ任意データ入力を発生し、

(iii)該第2の任意データ入力から第2のプロセッサデータ入力非可逆的変換を計算し、

(iv) 該通信ネットワークを介して該第1のプロセッサに対して該第2のプロセッサデータ入力非可逆的変換を通信し、

(v) 上記ステップ(i)および(iv)の後で、該通信ネットワークを介して該第1のプロセッサに対して該第2の任意データ入力を通信し、

(vi)該通信ネットワークを介して該第1のプロセッサから任意データを受信し、

(vii) 上記ステップ(vi)の後で、該第1のプロセッサデータ入力非可逆的変換を上記ステップ(vi)において受信された該任意データ判定入力と比較することを特徴とする装置。

【請求項23】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサデータ入力非可逆的変換又は該第2のプロセッサデータ入力非可逆的変換が、対応する任意データ入力の非可逆的変換に基づくものである装置。

【請求項24】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサが、該第2のプロセッサが該第1のプロセッサの該第1のプロセッサデータ入力を送信するのに先がけて該第1のプロセッサの第1のプロセッサデータ入力非可逆的変換を受信したことの確証を受信する装置。

【請求項25】 請求項21又は請求項22のいずれかに記載の装置において、

該第2のプロセッサが、該第1のプロセッサが該第1のプロセッサの該第2のプロセッサデータ入力を送るのに先がけて該第2のプロセッサの該第2のプロセッサデータ入力非可逆的変換を受信したという確証を受信する装置。

【請求項26】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサおよび該第2のプロセッサが、処理プロセス手法を用いて信頼性のある情報交換を確保するものである装置。

【請求項27】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサおよび該第2のプロセッサが、非拒絶手法を用いていずれの相手方も交換された情報を拒絶できないことを確保するものである装置。

【請求項28】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサおよび該第2のプロセッサが真贋の証明手法を用いて情報交換のプライバシーを確保するものである装置。

【請求項29】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサおよび該第2のプロセッサが、暗号化手法を用いて情報交換のプライバシーを確保するものである装置。

【請求項30】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサおよび該第2のプロセッサが、各々、同時的処理を開始するのに先がけて他のものにより用いられるべき非可逆的変換を確認するものである装置。

【請求項31】 請求項21又は請求項22のいずれかに記載の装置において、

該第1のプロセッサが、該処理および情報交換のログを記憶するものである装置。

【請求項32】 請求項21又は請求項22のいずれかに記載の装置において、

該第2のプロセッサが該処理および情報交換のログを記憶するものである装置。

【請求項33】 請求項21又は請求項22のいずれかに記載の装置において、

該データ入力、該プロセッサのソースデータ入力のハッシュ、非可逆的変換又は他の関数を含むものである装置。

【請求項34】 通信ネットワークを介して秘密データ処理を生成し確認するための装置であって、

(i) 第1のプロセッサ秘密任意データ入力を発生し、

(ii) 該第1のプロセッサ任意データ入力から第1のプロセッサデータ入力非可逆的変換を計算し、

(iii) 該第1のプロセッサデータ入力非可逆的変換を、該通信ネットワークを介して第2のプロセッサに対して通信し、および

(iv) 上記ステップ(i)および(iii)の後で、該第1の秘密任意データ入力を、該通信ネットワークを介して第2のプロセッサに対して通信するための第1のプロセッサを含むことを特徴とする装置。

【請求項35】 請求項34に記載の装置において、さらに

該データ入力非可逆的変換および該第1の秘密任意データ入力を受信し、および該非可逆的変換を通して該第1の秘密任意データ入力を処理してその結果を比較することにより該第1の秘密任意データ入力を確認する第2のプロセッサを含む装置。

【請求項36】 通信ネットワークを介して秘密データ処理を生成し確認するための装置であって、

(i)通信ネットワークを介して第1のプロセッサデータ入力非可逆的変換を受信し、

(ii)通信ネットワークを介して第1のプロセッサ秘密任意データ入力を受信し、

(iii)上記ステップ(i)および(ii)の後で、該第1のプロセッサデータ入力非可逆的変換を、該第2のプロセッサが計算する該第1のプロセッサ秘密任意データ入力の非可逆的変換と比較するための第2のプロセッサを含むことを特徴とする装置。

【請求項37】 請求項34に記載の装置において、さらに

該第1のプロセッサ任意データ入力を発生し、該第1のプロセッサデータ入力非可逆的変換を計算し、およびそれらを該通信ネットワークを介して該第2のプロセッサに提供する第1のプロセッサを含む装置。

【請求項38】 請求項35又は請求項37のいずれかに記載の装置において、

該第1および第2のプロセッサが、各々秘密データを発生しおよび確認する装置。

【請求項39】 請求項35又は請求項37のいずれかに記載の装置において、

該第1および第2のプロセッサが、そこで論理的に同一の処理を発生し、該第1および第2のプロセッサが、各々その秘密任意データ入力を提供するのに先立ち該通信ネットワークを介して他のプロセッサに対してそのそれぞれのデータ入力非可逆的変換を提供するようになっている装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 98/18047		
A. CLASSIFICATION OF SUBJECT MATTER IPC 6 G07F17/32		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 G07F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages Relevant to claim No.	
X A	WO 97 19537 A (WALKER ASSET MANAGEMENT) 29 May 1997 see page 1, line 5 - line 30 see page 6, line 4 - line 30 see page 7, line 30 - page 8, line 20 see page 22, line 29 - page 23, line 11; figures ---	19 1,8,13, 15
X A	WO 97 02073 A (WALKER ASSET MANAGEMENT) 23 January 1997 see page 11, line 13 - line 30 see page 20, line 4 - line 18; figures -----	19 1,8,13, 15
<input type="checkbox"/> Further documents are listed in the continuation of box C.		
<input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (see specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "B" document member of the same patent family		
Date of the actual completion of the international search 21 December 1998	Date of mailing of the international search report 04/01/1999	
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl Fax: (+31-70) 340-3016	Authorized officer Neville, D	

INTERNATIONAL SEARCH REPORT

Information on patent family members

 Inter: naf Application No
 PCT/US 98/18047

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9719537 A	29-05-1997	US 5768382 A	16-06-1998
		AU 1081997 A	11-06-1997
		EP 0862824 A	09-09-1998
WO 9702073 A	23-01-1997	AU 5285098 A	02-04-1998
		AU 6402396 A	05-02-1997
		AU 6405396 A	05-02-1997
		WO 9702074 A	23-01-1997

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

(72)発明者 キャンベル, シェリル, スーザン
アメリカ合衆国, 20009 ワシントン, デ
ィーシー, シックスティーンズ ストリー
ト, エヌ, ダヴリュ., 1837

Fターム(参考) 2C001 AA13 BB00 BB05 BB08 BD00
BD03 BD04 CB00 CB07 CB08
5B049 AA05 BB36 BB61 CC00 CC03
CC36 DD01 EE02 EE03 EE05
EE23 FF07 GG02 GG03 GG04
GG07 GG10

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第1部門第2区分

【発行日】平成17年9月15日(2005.9.15)

【公表番号】特表2001-514909(P2001-514909A)

【公表日】平成13年9月18日(2001.9.18)

【出願番号】特願2000-509065(P2000-509065)

【国際特許分類第7版】

A 6 3 F 13/12

A 6 3 F 13/00

G 0 6 F 17/60

【F I】

A 6 3 F 13/12 C

A 6 3 F 13/00 A

G 0 6 F 17/60 1 4 8

【手続補正書】

【提出日】平成15年12月26日(2003.12.26)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項1

【補正方法】変更

【補正の内容】

【請求項1】

通信ネットワークを通して、公正なゲーム進行手続を確認するための装置であって、ゲーム・シードを発生するためのホスト・プロセッサであって、衛星プロセッサからゲーム入力を受信し、前記ゲーム入力、ゲーム・シード、および予め定めたゲームの規則に基づいて、ゲームの結果を発生し、前記ゲーム・シードおよび前記ゲームの結果を前記衛星プロセッサに送信するホスト・プロセッサと、

前記通信ネットワークを介して、ホスト・プロセッサに前記ゲーム入力を提供し、前記ホスト・プロセッサから、前記ゲーム・シードおよび前記ゲームの結果を受信し、(i)前記ゲーム入力、前記ゲーム・シード、および前記の予め定めゲームの規則に基づいて、ゲームの結果を発生し、および(ii)前記の発生したゲームの結果を、前記の受信したゲームの結果とを比較することにより進行の公正を確保するための衛星プロセッサとを備える装置。